DG834GUv5 Wireless Router with Built-in DSL Modem User Manual

NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134-1911 USA

Broadband
Powered by Telkom

© 2009 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR and the NETGEAR logo are trademarks of Netgear, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. For product available in the USA market, only channels 1~11 can be operated. Selection of other channels is not possible

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DG834GUv5 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your

Telkom

Contents

Wireless ADSL2+ Modem Router DG834GUv5 User Manual

About This Manual

Conventions, Formats, and Scope xi
How to Use This Manual xii
How to Print this Manual xii

Chapter 1
Configuring Your Internet Connection

What You Need Before You Begin 1-1
Using the Smart Wizard to Set Up Your Router 1-2
Logging In to the Modem Router 1-3
Using the Setup Wizard to Auto-Detect Your Internet Connection 1-4
Viewing or Manually Configuring Your ISP Settings 1-6
Changing Your ADSL Settings 1-10
How the Internet Connection Works 1-11

Chapter 2
Configuring Your Wireless Network and Security Settings

Planning Your Wireless Network 2-1
Wireless Placement and Range Guidelines 2-2
Wireless Security Options 2-3
Manually Configuring Your Wireless Network 2-4
Configuring Your Wireless Security 2-7
Using Push 'N' Connect (WPS) to Configure Your Wireless Network 2-10
Using a WPS Button to Add a WPS Client 2-11
Using PIN Entry to Add a WPS Client 2-12
Connecting Additional Wireless Client Devices After WPS Setup 2-14
Advanced Wireless Settings for WPS and WDS 2-15
Controlling Wireless Station Access 2-16

Restricting Access by MAC Address 2-17

Chapter 3
Protecting Your Network

Protecting Access to Your ADSL2+ Modem Wireless Router 3-1
Changing the Built-In Password 3-1
Changing the Administrator Login Time-out 3-2
Configuring Basic Firewall Services 3-2
Blocking Keywords, Sites, and Services 3-3
Blocking Keywords and Sites 3-3
Firewall Rules 3-5
Inbound Rules (Port Forwarding) 3-6
Outbound Rules (Service Blocking) 3-8
Order of Precedence for Rules 3-10
Services 3-10
Setting Times and Scheduling Firewall Services 3-11
Scheduling Firewall Services 3-13

Chapter 4
Managing Your Network

Backing Up, Restoring, or Erasing Your Settings 4-1
Backing Up the Configuration to a File 4-1
Restoring the Configuration from a File 4-2
Erasing the Configuration 4-2
Upgrading the Modem Router Firmware 4-2
Network Management Information 4-4
Viewing Modem Router Status and Usage Statistics 4-4
Viewing Attached Devices 4-8
Viewing, Selecting, and Saving Logged Information 4-9
Log Message Examples 4-11
Enabling Security Event E-mail Notification 4-12
Running Diagnostic Utilities and Rebooting the Modem Router 4-13
Enabling Remote Management 4-14
Configuring Remote Management 4-14

Chapter 5
Advanced Configuration

Modifying Your WAN Setup 5-1

Setting Up a Default DMZ Server 5-3
Configuring Your LAN IP Settings 5-4
Using the Modem Router as a DHCP Server 5-6
Defining Reserved IP Addresses 5-7
Configuring Dynamic DNS 5-8
Using Static Routes 5-9
Static Route Example 5-9
Configuring Static Routes 5-10
Configuring Universal Plug and Play (UPnP) 5-11
Configuring Wireless Bridging and Repeating (WDS) 5-13
Point-to-Point Bridge Configuration 5-14
Multi-Point Bridge Configuration 5-15
Repeater with Wireless Client Association 5-17

Chapter 6
Configuring Telkom VPN Lite

What is VPN Lite? 6-1
Configuring VPN Lite 6-2

Chapter 7
Troubleshooting

Basic Functioning 7-1
Power LED Is Not On 7-2
Power LED Is Red 7-2
LAN or DSL or Internet Port LEDs Are Not On 7-2
Troubleshooting Access to the Modem Router Main Menu 7-2
Troubleshooting the ISP Connection 7-3
ADSL Link 7-3
ADSL Link 7-4
Obtaining a WAN IP Address 7-5
Troubleshooting PPPoE or PPPoA 7-6
Troubleshooting Internet Browsing 7-6
Troubleshooting a TCP/IP Network Using the Ping Utility 7-7
Testing the LAN Path to Your Router 7-7
Testing the Path from Your Computer to a Remote Device 7-8
Restoring the Default Configuration and Password 7-8
Problems with Date and Time 7-9

Appendix A
Technical Specifications

AppendixB
Related Documents

About This Manual

The *NETGEAR® DG834GUv5 Wireless Router with Built-in DSL Modem User Manual* describes how to install, configure, and troubleshoot the 54 Mbps Wireless ADSL2+ Modem Router with USBModel DG834GUv5. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
Italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.

	Tip: This format is used to highlight a procedure that will save time or resources.

	Warning: Ignoring this type of note might result in a malfunction or damage to the equipment.

- **Scope**. This manual is written for the ADSL2+ Modem Wireless Router according to these specifications:

Product Version	54 Mbps Wireless ADSL2+ Modem Router with USBModel DG834GUv5
Manual Publication Date	May 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in AppendixB , “Related Documents”.

Note: Product updates are available on the HCOM website at *http://www.hcom.co.za*

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forward or backward through the manual one page at a time.
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following options, according to your needs.

- **Printing a page in the HTML view**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a chapter**.

Use the *PDF of This Chapter* link at the top left of any page.

– Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

– Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at *http://www.adobe.com*.

– Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

• **Printing the full manual**.

Use the *Complete PDF Manual* link at the top left of any page.

– Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

– Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Configuring Your Internet Connection

This chapter describes how to configure your ADSL2+ Modem Wireless Router Internet connection. When you perform the initial configuration of your modem router using the *Resource CD* as described in the *NETGEAR Router Setup Manual,* these settings are configured automatically for you. This chapter provides further details about these settings, as well as instructions on how to log in to the modem router for further configuration.

	Note: NETGEAR recommends using the Smart Wizard on the *Resource CD* for initial configuration, as described in the *NETGEAR Wireless ADSL2+ Modem Router Setup Manual*.

This chapter includes:

- "Logging In to the Modem Router"
- "Using the Installation CD to Set Up Your Router"
- "Logging In to the Modem Router"
- "Viewing or Manually Configuring Your ISP Settings"
- "Changing Your ADSL Settings"
- "How the Internet Connection Works"

What You Need Before You Begin

You need to prepare the following before you can set up your ADSL2+ Modem Wireless Router:

- Active Internet service provided by an ADSL account.
- The Internet Service Provider (ISP) configuration information for your ADSL account.
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
  - Host and domain names
- ASDL microfilters as explained in the *Installation CD or the printed Qhick Install Guide*.

- Your computer must be set up to use DHCP to get its TCP/IP configuration from the modem router. This is usually the case. For help with DHCP, see the documentation that came with your computer, or see the link to the online document in “Preparing a Computer for Network Access” in Appendix B .

Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.

Using the Installation CD to Set Up Your Router

For first-time installation of your modem router, Netgear recommends using the Installation CD. The Installation CD will assist you to connect your router and computers. The Smart Wizard application on the Intallation CD will assist you in configuring your device to connect to the internet, configure wireless settings and wireless security, setup email and tests all the relevant settings. After initial configuration using the Installation CD, you can use the information in this Reference Manual to configure additional features of your wireless router.

.

Note: The Smart Wizard cannot detect a PPTP connection with your ISP. If your ISP uses this protocol, then you must configure your connection manually (see “Viewing or Manually Configuring Your ISP Settings” on page 1-3).

Logging In to the Modem Router

You can log in to the modem router to view or change its settings.

Note: Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in “Preparing a Computer for Network Access” in Appendix B .

To log in to the modem router:

1. Type **http://routerlogin.net** or **http://10.0.0.2** in the address field of an Internet browser.

Figure 1-1

This login window opens:

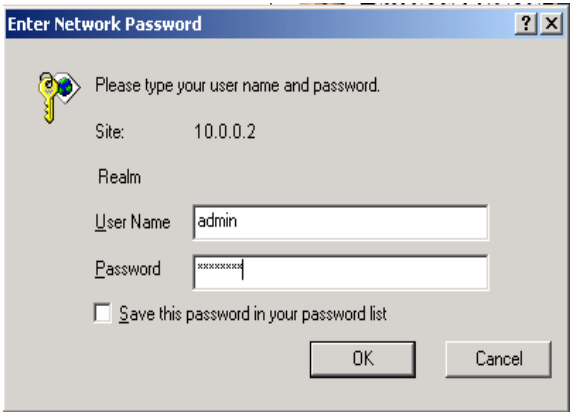


Figure 1-2

2. Enter **admin** for the user name and **admin** for the password, both in lower case letters.
3. Click **OK.** You will be logged in to your router's main menu.

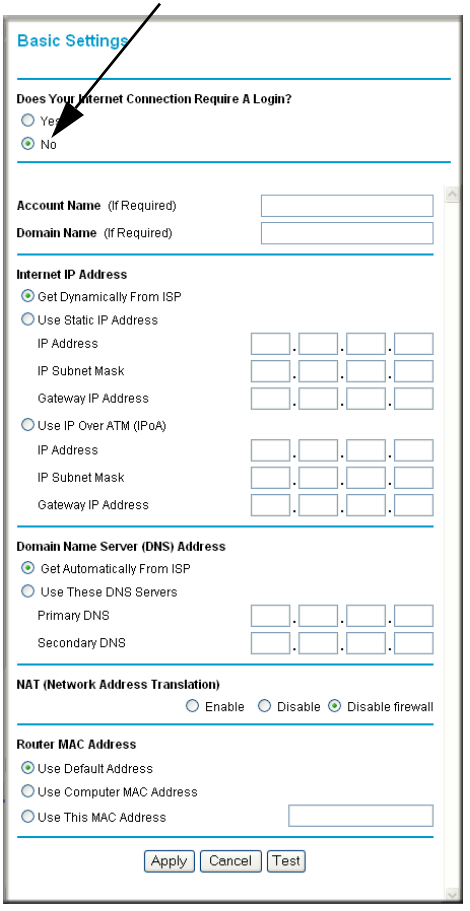
Viewing or Manually Configuring Your ISP Settings

NETGEAR recommends that you specify your country and language before you configure the settings on the Basic Settings screen. See "Logging In to the Modem Router" on page 1-2. You must install the ADSL filters and connect the modem router to the ADSL line as described in the *NETGEAR Router Setup Manual* before you configure the settings in the Basic Settings screen.

To view or configure the basic settings:

1. Log in to the modem router as described in "Logging In to the Modem Router".
2. Select Basic Settings to display the Basic Settings screen.

ISP *does not* require login



ISP *does* require login

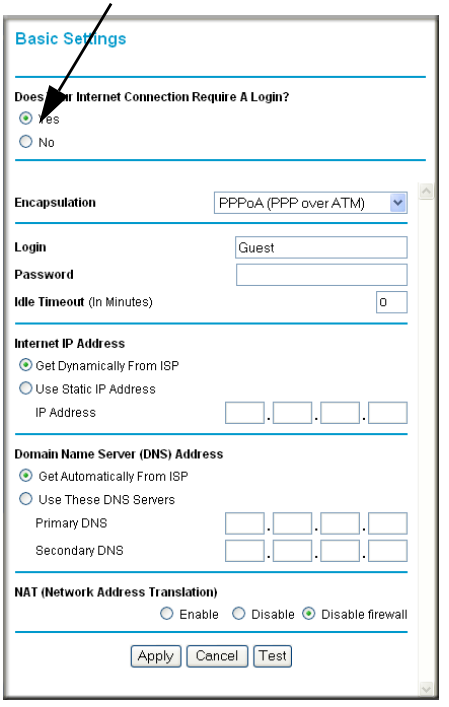


Figure 1-3

The fields on the Basic Settings screen depend on whether or not your Internet connection requires a login. The Basic Settings screen is explained in Table 1-1. “Basic Settings Fields Description”.

3. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.

   - **Yes**. If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.

4. Enter the settings for the IP address and DNS server.

   The default ADSL settings usually work fine. If you have problems with your connection, check the ADSL settings. See "Changing Your ADSL Settings" for more details.

5. If no login is required, you can specify the MAC Address setting.

6. Click **Apply** to save your settings.

7. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

Note: When your Internet connection is working you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in.

Table 1-1. Basic Settings Fields Description

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields appear only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields appear only if your ISP requires a login.	Encapsulation	• PPPoE • PPPoA • PPTP
	Login	The login name provided by your ISP. This is often an e-mail address.
	Idle Timeout (In minutes)	If you want to change the login time-out, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.

Table 1-1. Basic Settings Fields Description

Settings	Description
Internet IP Address	• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's modem router to which your modem router will connect. • **Use IP Over ATM (IFoA)**. Your ISP uses Classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.
Domain Name Server (DNS) Address	The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. • **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
NAT (Net Address Translation)	NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices. • **Enable**. Usually NAT is enabled. • **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the DG834GUv5 uses. Classical routing should be selected only by experienced users.[a] • **Disable Firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.

Table 1-1. Basic Settings Fields Description

Settings		Description
This field appears only if no login is required.	Router MAC Address	The Ethernet MAC address that will be used by the modem router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your modem router to masquerade as that computer by "cloning" its MAC address. • **Use Default Address**. Use the default MAC address. • **Use Computer MAC Address**. The modem router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • **Use This MAC Address**. Enter the MAC address that you want to use.

a. Disable NAT only if you plan to install the modem router in a setting where you will be manually administering the IP address space on the LAN side of the router.

Changing Your ADSL Settings

Note: For information about how to install ADSL filters, see the *NETGEAR Router Setup Manual*.

The default ADSL settings of your modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

Note: You must use the Setup Wizard to select the correct country for the default ADSL settings to work. The default settings are set for Telkom ADSL.

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting:

1. From the main menu, select **ADSL Settings**.
2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**. The default is **LLC-based**.

3. Type a number between 0 and 255 for the VPI. The default is 8.
4. Type a number between 32 and 65535 for the VCI. The default is 35.
5. Click **Apply**.

How the Internet Connection Works

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as dial-up networking or Enternet to connect, log in, or disconnect. The modem router performs these functions automatically as needed.

To access the Internet from any computer connected to your modem router, launch an Internet browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the modem router's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

Chapter 2
Configuring Your Wireless Network and Security Settings

For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

	Warning: Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- "Planning Your Wireless Network"
- "Manually Configuring Your Wireless Network" on page 2-4
- "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10
- "Advanced Wireless Settings for WPS and WDS" on page 2-15
- "Controlling Wireless Station Access" on page 2-16
- "Restricting Access by MAC Address" on page 2-17

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the modem router is printed on the belly label of your modem for example: DO_123456.
  - The wireless mode (802.11g, or 802.11b) that each wireless adapter supports.

– Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See "Manually Configuring Your Wireless Network" on page 2-4.

- Push 'N' Connect (WPS) automatically implements wireless security on the modem router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the modem router, clicking an onscreen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

  To set up your wireless network using the WPS feature:

  – Use the WPS button on the side of the modem router (there is also an onscreen WPS button), or enter the PIN of the wireless device.

  – Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

  See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the modem router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your modem router according to the following guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The ADSL2+ Modem Wireless Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

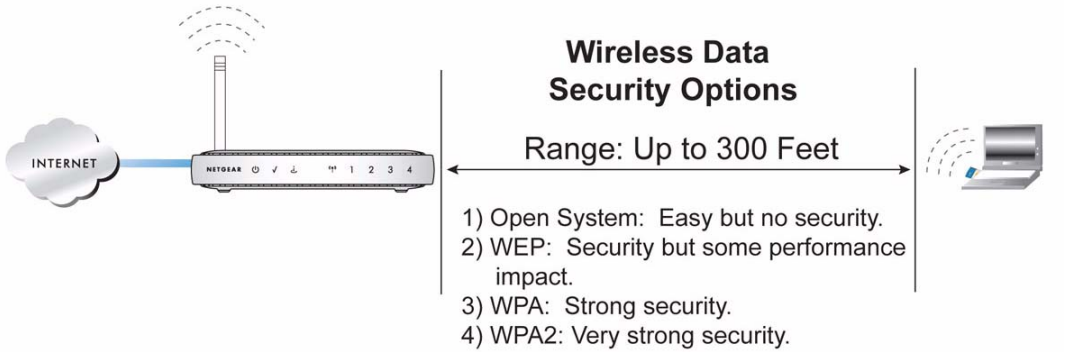

Wireless Data
Security Options
Range: Up to 300 Feet
INTERNET
1) Open System: Easy but no security.
2) WEP: Security but some performance impact.
3) WPA: Strong security.
4) WPA2: Very strong security.

Figure 2-1

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK (see “Configuring WEP” on page 2-8)..
- **WPA-802.1x, WPA2-802.1x**. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise“Configuring WPA, WPA2, or WPA/WPA2” on page 2-9).

You also can increase your security by implementing one or more of the following features:

- **Restrict Access Based on MAC Address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the modem router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed (see "Restricting Access by MAC Address" on page 2-17).
- **Turn Off the Broadcast of the Wireless Network Name SSID**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network 'discovery' feature of some products, such as Windows XP, but the data is still exposed (see "Controlling Wireless Station Access" on page 2-16).

For more information about wireless technology, see the link to the online document in "Wireless Communications" in Appendix B .

Manually Configuring Your Wireless Network

You can view or manually configure the wireless settings and wireless security for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.

	Note: If you use a wireless computer to change the wireless network name (SSID) or wireless security settings, you will be disconnected when you click **Apply**. To avoid this problem, use a computer with a wired connection to access the modem router.

To manually configure the wireless settings:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, and default password of **admin**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. Select Wireless Settings from the main menu to display the Wireless Settings screen:

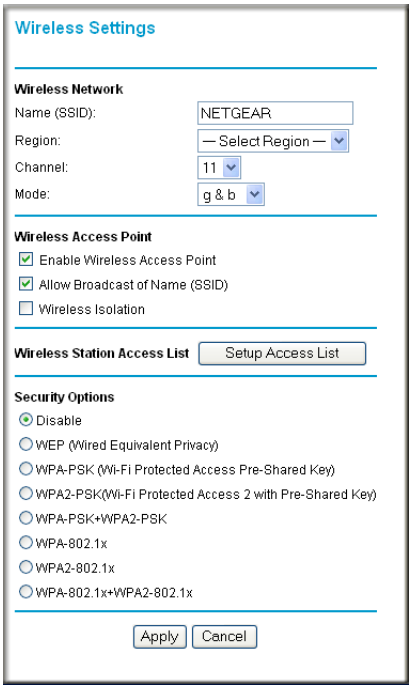


Figure 2-2

The settings for this screen are explained in Table 2-1 on page 2-6.

3. Select the region in which the modem router will operate.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.
6. Configure and test your computers for wireless connectivity. After testing your wireless connectivity, select a security method (see "Configuring Your Wireless Security" on page 2-7).

   Program the wireless adapter of your computers to have the same SSID and wireless security settings as your modem router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the modem router. If there is interference, adjust the channel.

Table 2-1. Wireless Settings

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a wireless network must use the SSID.
	Region	The location where the Product Family is used.
	Channel	The wireless channel used by the gateway. The default is Channel 6. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
	Mode	The default is g & b, which allows both 802.11g and 802.11b wireless stations access. Note that in b only mode, 802.11g wireless stations can connect if they can operate in 802.11b mode.
Wireless Access Point	Enable Wireless Access Point	Selected by default, this setting enables the wireless radio, which allows the modem router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.
	Allow Broadcast Name (SSID)	Selected by default, the modem router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of products such as Windows XP, but the data is still exposed to equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.
	Wireless Isolation	This feature is disabled by default. If it is enabled, wireless stations cannot communicate with each other or with stations on the wired network.
Wireless Station Access List	Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect. See “Restricting Access by MAC Address”.

Table 2-1. Wireless Settings (continued)

Settings	Description
Security Options (see "Configuring Your Wireless Security").	• **Disabled**. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy)**. Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See "Configuring WEP". • **WPA-PSK (WiFi Protected Access Pre-Shared Key).** Allow only computers configured with WPA to connect to the modem router. See "Configuring WPA, WPA2, or WPA/WPA2". • **WPA2-PSK (Wi-Fi Protected Access with 2 Pre-Shared Keys)**. Allow only computers configured with WPA2 to connect to the modem router. See "Configuring WPA, WPA2, or WPA/WPA2"**.** • **WPA-PSK + WPA2-PSK**. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the modem router. See "Configuring WPA, WPA2, or WPA/WPA2". • The **WPA-802.1x**, **WPA2-802.1**, and **WPA-802.1x +WPA2-802.1** options utilize user authentication implemented using IEE 802.1x and Radius servers. See "Configuring WPA, WPA2, or WPA/WPA2".

Configuring Your Wireless Security

To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

Configuring WEP

To configure WEP data encryption:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, and default password of **admin**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. From the main menu, select Wireless Settings to display the Wireless Settings screen.
3. In the Security Options section, select the **WEP (Wired Equivalent Privacy)** radio button:

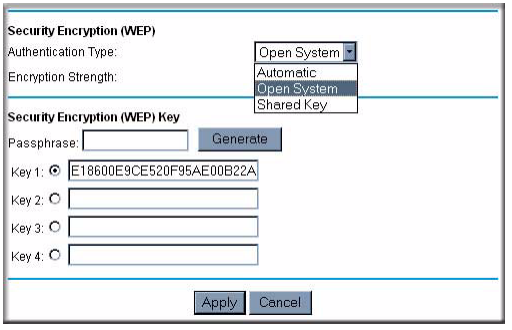


Figure 2-3

4. Select the **Authentication Type**: **Automatic**, **Open System**, or **Shared Key**. The default is Open System.

	Note: The authentication scheme is separate from the data encryption. You can select an authentication scheme that requires a shared key but still leaves the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

5. Select the **Encryption Strength** setting:
   - **WEP (Wired Equivalent Privacy) 64-bit encryption**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
   - **WEP (Wired Equivalent Privacy) 128-bit encryption**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network:

- **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the modem router.

  Note: Not all wireless adapters support passphrase key generation.

- **Key 1-Key4**. These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

7. Select which of the four keys will be the default.

   Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.

8. Click **Apply** to save your settings.

Configuring WPA, WPA2, or WPA/WPA2

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later; WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. If this happens, reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

To configure WPA or WPA2 in the modem router:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** and default password of **admin**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. Select Wireless Settings from the main menu.
3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.
4. The settings displayed on the screen depend on which security option you select.

5. For WPA-PSK or WPA2-PSK, enter the passphrase.
6. If prompted, enter the settings for the Radius server. For WPA-802.1x or WPA2-802.1x, these settings are required for communication with the primary Radius server.
   - **Primary Radius Server IP Address**. The IP address of the Radius server. The default is 0.0.0.0
   - **Radius Port**. Port number of the Radius server. The default is 1812.
   - **Shared Key**. This is shared between the wireless access point and the Radius server during authentication.
7. To save your settings, click **Apply**.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the modem router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the modem router. Look for the symbol on your client device (computers that will connect wirelessly to the modem router are clients). WPS automatically configures the network name (SSID) and wireless security settings for the modem router (if the modem router is in its default state) and broadcasts these settings to the wireless client.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.
- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices. See "Connecting Additional Wireless Client Devices After WPS Setup" on page 2-14.

A WPS client can be added using the Push Button method or the PIN method.

- **Using the Push Button**. This is the preferred method. See the following section, "Using a WPS Button to Add a WPS Client".

- **Entering a PIN**. For information about using the PIN method, see "Using PIN Entry to Add a WPS Client" on page 2-12.

Using a WPS Button to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the modem router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

To use the modem router WPS button to add a WPS client:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** and default password of **admin**, or using whatever LAN address and password you have set up.
2. On the modem router main menu, select Add a WPS Client, and then click **Next**. The following screen displays:

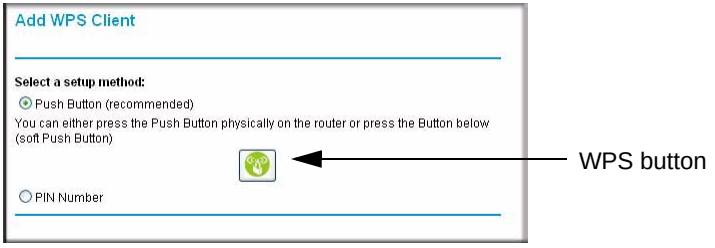

Add WPS Client
Select a setup method:
Push Button (recommended)
You can either press the Push Button physically on the router or press the Button below (soft Push Button)
PIN Number
WPS button

Figure 2-4

By default, the **Push Button (recommended)** radio button is selected.

3. Either press the WPS button on the side of the modem router, or click the onscreen button.

   The modem router tries to communicate with the client for 2 minutes.

4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
5. Go back to the modem router screen to check for a message.

   The modem router WPS screen displays a message confirming that the client was added to the wireless network. The modem router generates an SSID, and implements WPA/WPA2

wireless security. The modem router will keep these wireless settings unless you change them, or you clear the **Keep Existing Wireless Settings** check box in the WPS Settings screen.

Figure 2-5

6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the modem router's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute timeframe, the SSID will not be changed, and no security will be implemented on the modem router.

Using PIN Entry to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the modem router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the modem router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use a PIN to add a WPS client:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** and default password of **admin**, or using whatever LAN address and password you have set up.

2. On the modem router main menu, select Add a WPS Client (computers that will connect wirelessly to the modem router are clients), and then click **Next**. The Add WPS Client screen displays:

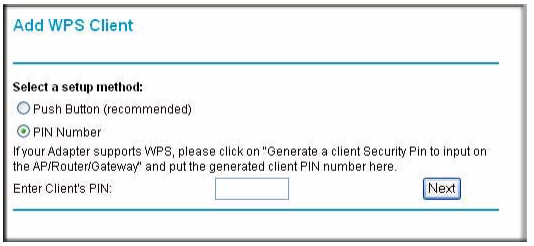

Add WPS Client
Select a setup method:
Push Button (recommended)
PIN Number
If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.
Enter Client's PIN:
Next

Figure 2-6

3. Select the **PIN Number** radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. From the modem router Add WPS Client screen, enter the client PIN number, and then click **Next**.
   - The modem router tries to communicate with the client for 4 minutes.
   - The modem router WPS screen displays a message confirming that the client was added to the wireless network. The modem router generates an SSID, and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the modem router's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute timeframe, the SSID will not be changed and no security will be implemented on the modem router.

Connecting Additional Wireless Client Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** checkbox is selected in the Advanced Wireless screen (listed under the Advanced heading in the modem router main menu). If you clear this checkbox, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the modem router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in "Using a WPS Button to Add a WPS Client" on page 2-11 or "Using PIN Entry to Add a WPS Client" on page 2-12.
2. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see "Viewing Attached Devices" on page 4-8.

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the modem router:

1. Restore the modem router to its factory default settings (press both the Wireless and WPS buttons on the side of the modem router for 5 seconds).

   When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the modem router.
2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10). and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
4. For the WPS devices that you want to connect, follow the procedure "Using a WPS Button to Add a WPS Client" on page 2-11 or "Using PIN Entry to Add a WPS Client" on page 2-12.

The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the modem router.

	Note: To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the WPS Settings screen.

5. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see "Viewing Attached Devices" on page 4-8.

Advanced Wireless Settings for WPS and WDS

The Advanced Wireless Settings screen includes settings for Push 'N' Connect (WPS) and for Wireless Distribution System (WDS) setup. From the main menu, select Advanced Wireless Settings to display the following screen:

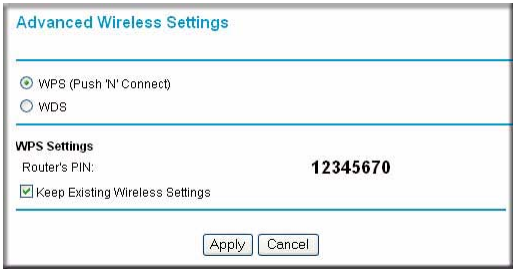


Figure 2-7

- **WPS (Push 'N' Connect)**. The WPS settings show the modem router PIN, and the **Keep Existing Wireless Settings** check box.

  By default, the **Keep Existing Wireless Settings** check box is cleared. This allows the modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

  If you configure your wireless router settings and security manually, the **Keep Existing Wireless Settings** radio box will also be enabled. This will allow you to use WPS (Push 'N' Connect) to connect additional WPS capable devices to your wireless network using the existing settings.

- **WDS**. Select this radio button to configure a wireless distribution system (WDS). You can build large bridged wireless networks. See "Configuring Wireless Bridging and Repeating (WDS)" in Chapter 5.

Controlling Wireless Station Access

By default, any wireless PC that is configured with the correct SSID and wireless security settings is allowed access to your wireless network. You can use Wireless Access Point settings in the Wireless Setting screen to further restrict wireless access to your network:

Figure 2-8

- **Turning off wireless connectivity completely**.
  You can completely turn off the wireless portion of the modem router. For example, if you use your notebook computer to wirelessly connect to your modem router, and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router via Ethernet cables can still use the modem router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.
- **Hiding your wireless network name (SSID)**.
  By default, the modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Allow Broadcast of Name (SSID)** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not "see" your modem router. You must configure your wireless devices to match the wireless network name (SSID) of the modem router.

	Note: The SSID of any wireless access adapters must match the SSID you configure in the modem router. If they do not match, you will not get a wireless connection to the modem router.

Restricting Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the ADSL2+ Modem Wireless Router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

To restrict access based on MAC addresses:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, and default password of **admin**, or using whatever user name, password, and LAN address you have chosen for the modem router.

> **Note:** If you configure the Product Family from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

2. From the main menu, select Wireless Settings, and then click **Setup Access List** to display the Wireless Station Access List screen.

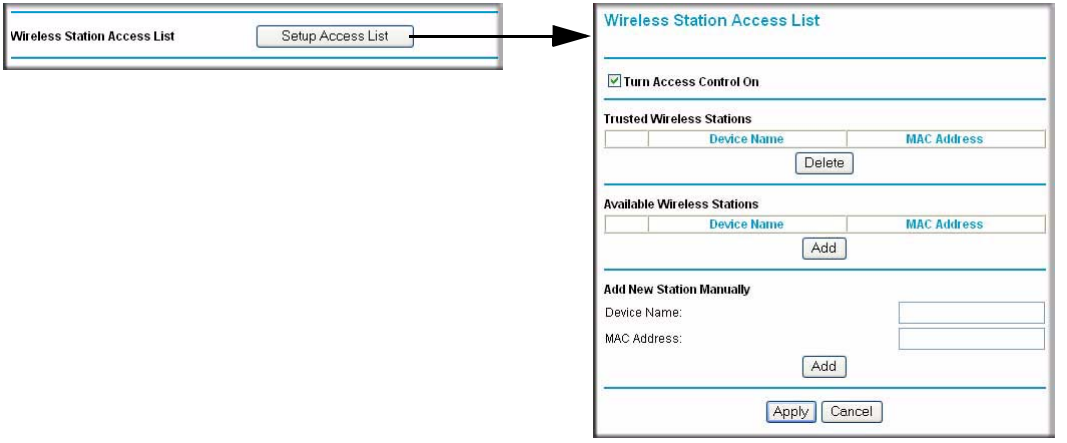


Figure 2-9

The trusted wireless stations listed on this screen are the wireless clients that will have access to the wireless network when the list is enabled.

3. Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list using either of the following methods:

   - If the computer is in the Available Wireless Stations table, select the radio button of that computer to capture its MAC address.
   - Use the Add New Station Manually fields to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device.

Note: If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding.

4. Click **Add**, and then click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the Product Family.

Chapter 3
Protecting Your Network

This chapter describes how to use the basic firewall features of the ADSL2+ Modem Wireless Router to protect your network.

Protecting Access to Your ADSL2+ Modem Wireless Router

For security reasons, the modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the modem router user name and **admin** for the modem router password. You can use procedures in the following sections to change the modem router password and the amount of time for the administrator's login time-out.

Note: The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Built-In Password

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.

2. From the main menu, under the Maintenance heading, select Set Password to display the Set Password screen:

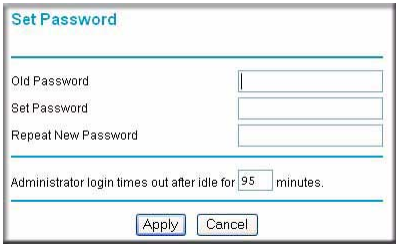


Figure 3-1

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

	Note: After changing the password, you must log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password.

Changing the Administrator Login Time-out

For security, the administrator login to the modem router configuration times out after a period of inactivity. To change the login time-out period:

1. In the Set Password screen, type a number in the **Administrator login times out** field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.

Configuring Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented in the following sections.

Blocking Keywords, Sites, and Services

The modem router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the modem router prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for keywords within Web addresses. Content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound service blocking. Limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Detects and thwarts denial of service (DoS) attacks such as Ping of Death, SYN flood, LAND attack, and IP spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

The following section explains how to configure your modem router to perform these functions.

Blocking Keywords and Sites

The modem router allows you to restrict access to Internet content based on Web addresses and Web address keywords.

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, and default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.
2. On the main menu, select Block Sites to display the Block Sites screen:

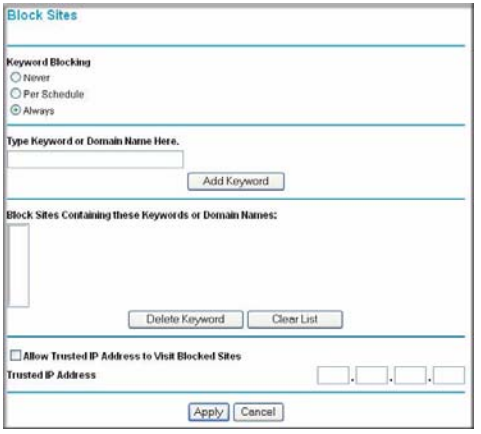


Figure 3-2

3. To enable keyword blocking, select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings on the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the setting in the Schedule screen.
4. Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

   Some examples of keyword applications are shown in the following chart.

Keyword	Result
XXX	Block the URL http://www.badstuf.com/xxx.html.
.com	Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
. (a period)	Block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.

> **Note:** If you block sites, you can set up the modem router to log attempts to access them. See "Viewing, Selecting, and Saving Logged Information" on page 4-9.

5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and then click **Apply**.

   You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.
7. Click **Apply** to save your settings.

Firewall Rules

Firewall rules block or allow specific traffic passing through from one side of the modem router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

The default inbound and outbound rules of the modem router are:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See "Order of Precedence for Rules" for more details.

To view or change firewall rules, select Firewall Rules on the main menu.

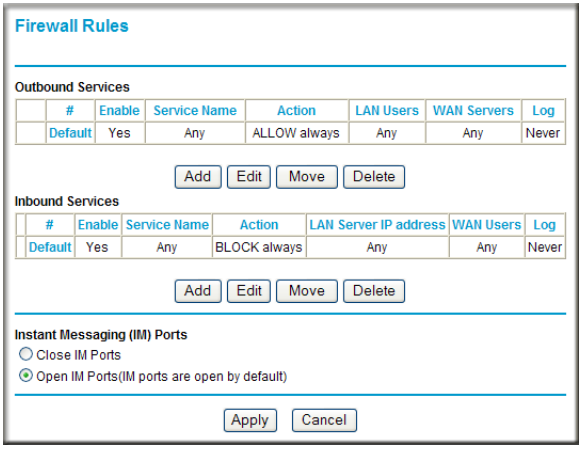

Firewall Rules
Outbound Services
Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always Any Any Never
Add Edit Move Delete
Instant Messaging (IM) Ports
Close IM Ports
Open IM Ports(IM ports are open by default)
Apply Cancel

Figure 3-3

- To edit an existing rule, select its button on the left side of the table and click **Edit**.
- To delete an existing rule, select its button on the left side of the table and click **Delete**.
- To move a rule to a different position in the table, select its button, and then click **Move**. At the prompt, enter the number of the desired new position, and then click **OK**.

Inbound Rules (Port Forwarding)

Because the modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly access any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

	Note: Some broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active services at your location. If you are unsure, see the acceptable use policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. Following are two application examples of inbound rules.

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from outside IP addresses to the IP address of your Web server at any time of day. This rule is shown in the following figure:

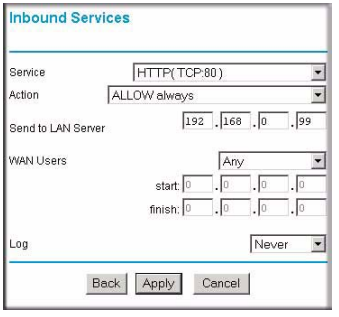


Figure 3-4

The settings are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear.

- **Action**. Select when you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule screen.
- **Send to LAN Server**. Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.
- **WAN Users**. These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must enter the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the rule will be logged.
  - **Not match**. Traffic of this type that does not match the rule will be logged.

Inbound Rule Example: Allowing Videoconferencing

You can create an inbound rule to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In this example, CU-SeeMe connections are allowed only from a specified range of external IP addresses. This example also specifies logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

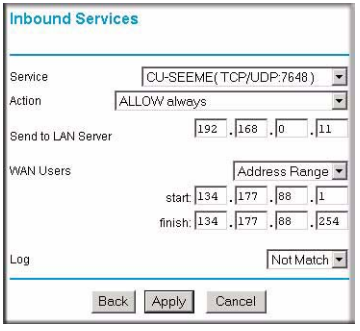


Figure 3-5

Considerations for Inbound Rules

If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature so that external users can always find your network.

If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.

Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the previous example). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The modem router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on the following:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule screen. You can also have the modem router log any attempt to use Instant Messenger during that blocked period.

The following screen shows AIM selected in the **Service** list:

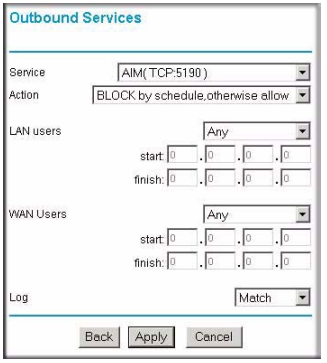


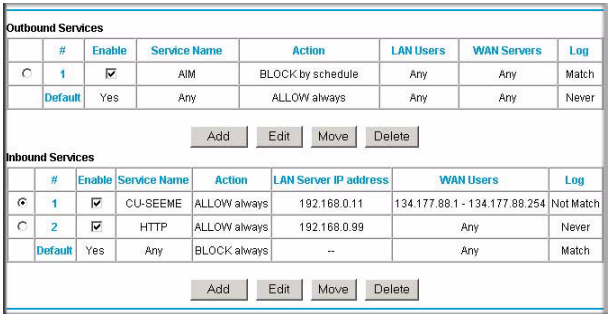
Figure 3-6

The Outbound Services screen includes the following fields:

- **Service**. Select the application or service from the drop-down list to be allowed or blocked. You can use the Add Custom Service feature to add any additional services or applications that are not in the list; see "Services" for details.
- **Action**. Choose when you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule defined in the Schedule screen.
- **LAN users**. This setting determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the Start field.
- **WAN users**. This setting determines which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.
- **Log**. Select whether the traffic will be logged. The choices are:
  - **Never**. No log entries will be made for this service.
  - **Always**. Any traffic for this service type will be logged.
  - **Match**. Traffic of this type that matches the rule will be logged.
  - **Not match**. Traffic of this type that does not match the rule will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Firewall Rules screen, as shown:



Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

Add Edit Move Delete

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
◉	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

Add Edit Move Delete

Figure 3-7

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the rules table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the modem router already holds a list of many service port numbers, you are not limited to these choices. Use the following procedure to define your own services.

To define a service:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.
2. Under the Content Filtering heading, select Services to display the Services screen:

Figure 3-8

- To create a new service, click **Add Custom Service**.
- To edit an existing service, select its button on the left side of the table, and then click **Edit Service**.
- To delete an existing service, select its button on the left side of the table, and then click **Delete Service**.

3. Use the screen shown in the following figure to define or edit a service.

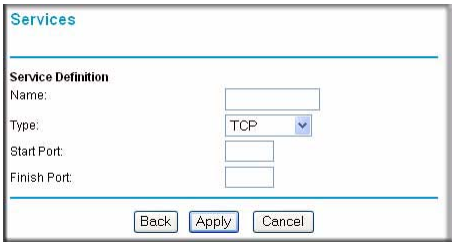


Figure 3-9

4. Click **Apply** to save your changes.

Setting Times and Scheduling Firewall Services

The modem router uses network time protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

To localize the time for your log entries, you must specify your time zone:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin**, default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.
2. On the main menu, select Schedule to display the Schedule screen:

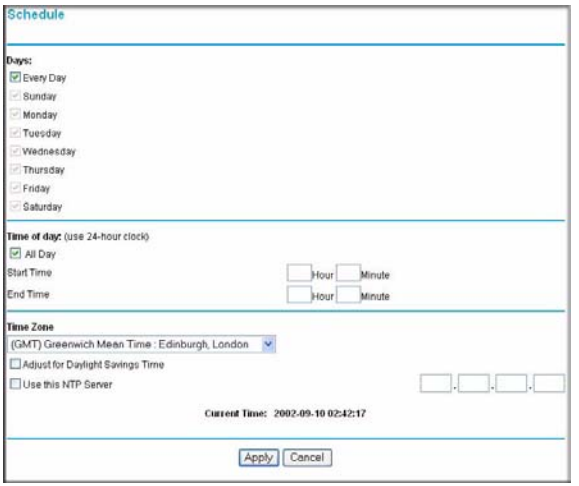


Figure 3-10

3. Select your time zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

   If your time zone is currently in daylight savings time, select the **Adjust for daylight savings time** check box.

	Note: If your region uses daylight savings time, you must manually select **Adjust for Daylight Savings Time** on the first day of daylight savings time, and clear it at the end. Enabling daylight savings time causes 1 hour to be added to the standard time.

4. The modem router has a list of TELKOM NTP servers. If you prefer to use a particular NTP server as the primary server, enter its IP address in the **Use this NTP Server** field.
5. Click **Apply** to save your settings.

Scheduling Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.
2. On the main menu, select the Schedule. The Schedule screen appears.
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, fill in the **Start Blocking** and **End Blocking** fields.
4. Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.
5. Click **Apply** to save your changes.

Chapter 4
Managing Your Network

This chapter describes how to perform network management tasks with your ADSL2+ Modem Wireless Router.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the modem router are stored in a configuration file in the modem router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

Backing Up the Configuration to a File

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.
2. Under the Maintenance heading on the main menu, select Backup Settings to display the Backup Settings screen:

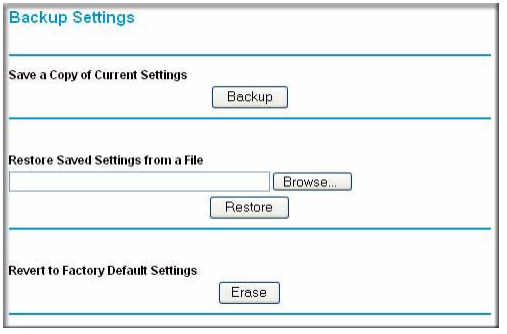


Figure 4-1

3. Click **Backup** to save a copy of the current settings.
4. Store the .cfg file on a computer on your network.

Restoring the Configuration from a File

To restore the configuration:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.
2. Under the Maintenance heading on the main menu, select Backup Settings.
3. Enter the full path to the file on your network, or click **Browse** to locate the file.
4. When you have located the .cfg file, click **Restore** to upload the file to the modem router.
5. The modem router reboots.

Erasing the Configuration

You can use the Erase feature to erase its configuration settings and restore the modem router to the factory default settings.

To erase the configuration:

1. Under the Maintenance heading on the main menu select, Backup Settings.
2. Click **Erase**.
3. The modem router reboots.

   After an erase, the modem router password is **admin**, the LAN IP address is **10.0.0.2**, and the modem router DHCP client is enabled.

	Note: To restore the factory default configuration settings when you do not know the login password or IP address, press both the Wireless button and WPS button on the side of the modem router for 5 seconds.

Upgrading the Modem Router Firmware

The software of the modem router is stored in flash memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR website. If the upgrade file is compressed (a .zip file), you must first extract the binary (.bin or .img) file before uploading it to the modem router.

NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might need to restore your configuration settings.

To upgrade the modem firmware:

1. Download and unzip the new software file from NETGEAR.

   The Web browser used to upload new firmware into the modem router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or later, or Mozilla Firefox 2.0 or later.

2. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.

3. From the main menu, under the Maintenance heading, select Router Upgrade to display the Firmware Upgrade screen:

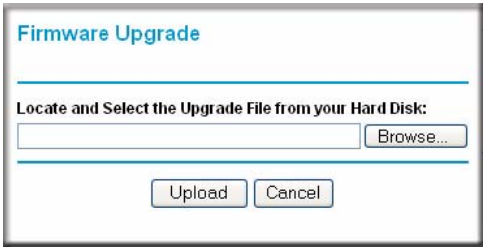


Figure 4-2

4. Click **Browse** to locate the binary (.bin or .img) upgrade file.

5. Click **Upload**.

⚠	**Warning:** When uploading software to the modem router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it might corrupt the software, causing modem router to be unworkable and inaccessible. When the upload is complete, your modem router will automatically restart. The upgrade process typically takes about 1 minute. In some cases, you might need to clear the configuration and reconfigure the modem router after upgrading.

Network Management Information

The modem router provides a variety of status and usage information which is discussed below.

Viewing Modem Router Status and Usage Statistics

From the main menu, below the Maintenance heading, select Router Status to view this screen.

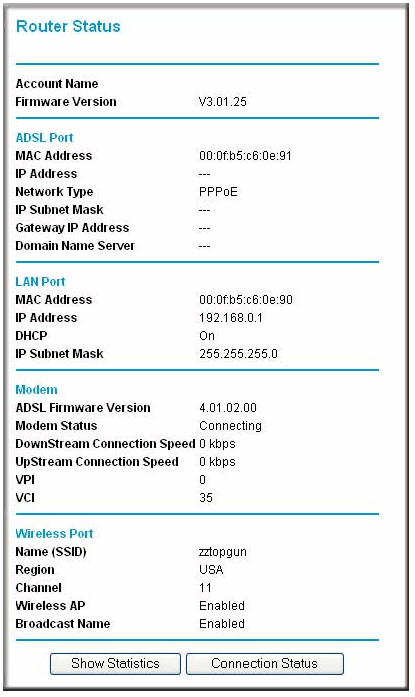


Figure 4-3

The Router Status screen provides status and usage information. This screen shows the following parameters:

Table 4-1. Modem Router Status Fields

Field	Description
Account Name	The host name assigned to the modem router in the Basic Settings screen.
Firmware Version	This field displays the modem router firmware version.

Table 4-1. Modem Router Status Fields (continued)

Field		Description
ADSL Port	MAC Address	The Ethernet MAC address used by the ADSL port of the modem router.
	IP Address	The IP address used by the ADSL port. If no address is shown, the modem router cannot connect to the Internet.
	Network Type	The network type is determined by your ISP. Common network types are PPPoE and PPPoA.
	IP Subnet Mask	The IP subnet mask used by the ADSL port.
	Domain Name Server (DNS)	The DNS server IP addresses used by the modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Ethernet MAC address used by the local (LAN) port of the modem router.
	IP Address	The IP address used by the local (LAN) port. The default is 10.0.0.2.
	DHCP	• **Off:** The modem router will not assign IP addresses to PCs on the LAN. • **On:** The modem router assigns IP addresses to PCs on the LAN.
	IP Subnet Mask	The IP subnet mask used by the local (LAN) port. The default is 255.255.255.0.
Modem	ADSL Firmware Version	The version of the firmware.
	Modem Status	The connection status of the modem.
	Downstream Speed	The speed at which the modem is receiving data from the ADSL line.
	Upstream Speed	The speed at which the modem is transmitting data to the ADSL line.
	VPI	The virtual path identifier setting.
	VCI	The virtual channel identifier setting.

Table 4-1. Modem Router Status Fields (continued)

Field		Description
Wireless Port These are set in the Wireless Settings page; see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.	Name (SSID)	The service set ID, also known as the wireless network name.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off.
	Broadcast Name	Indicates if the DG834GUv5 is configured to broadcast its SSID.

Viewing Statistics

Click the **Show Statistics** button on the Router Status screen to display modem router usage statistics:

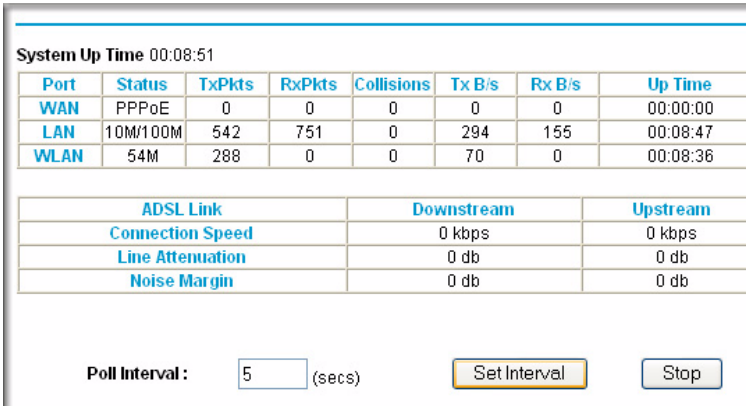

System Up Time 00:08:51
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN PPPoE 0 0 0 0 0 00:00:00
LAN 10M/100M 542 751 0 294 155 00:08:47
WLAN 54M 288 0 0 70 0 00:08:36
ADSL Link Downstream Upstream
Connection Speed 0 kbps 0 kbps
Line Attenuation 0 db 0 db
Noise Margin 0 db 0 db
Poll Interval : 5 (secs) Set Interval Stop

Figure 4-4

This following table explains the statistic fields.

Table 4-2. Router Statistics Fields

Field		Description
WAN (Internet), LAN, or WLAN (Wireless LAN) statistics	Status	The link status of the port.
	TxPkts	The number of packets transmitted on this port since reset or manual clear.
	RxPkts	The number of packets received on this port since reset or manual clear.
	Collisions	The number of collisions on this port since reset or manual clear.
	Tx B/s	The average egress line utilization for this port.
	Rx B/s	The average ingress line utilization for this port.
	Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream These statistics might help your technical support representative if there is a connection problem.	Connection Speed	Typically, the downstream speed is faster than the upstream speed.
	Line Attenuation	The line attenuation increases the further you are physically located from your ISP's facilities.
	Noise Margin	This is the signal-to-noise ratio and is a measure of the quality of the signal on the line.
	Poll Interval	Specifies the interval at which the statistics are updated in this window. Click **Stop** to freeze the display.

Viewing Connection Status

Click the **Connection Status** button on the Router Status screen to view the connection status:

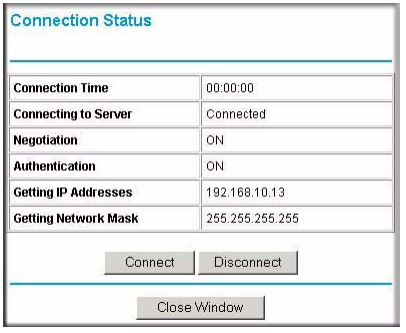


Figure 4-5

This screen shows the following statistics:

Table 4-3. Connection Status Fields for PPPoA

Field	Description
Connection Time	The time elapsed since the last connection to the Internet via the ADSL port.
Connecting to Sender	The connection status.
Negotiation	Success or Off.
Authentication	Success or Off.
IP Address	The IP address assigned to the WAN port by the ADSL Internet Service Provider.
Network Mask	The network mask assigned to the WAN port by the ADSL Internet Service Provider.

Viewing Attached Devices

The Attached Devices screen contains a table of all IP devices that the modem router has discovered on the local network. From the main menu, under the Maintenance heading, select Attached Devices. The Attached Devices screen displays:

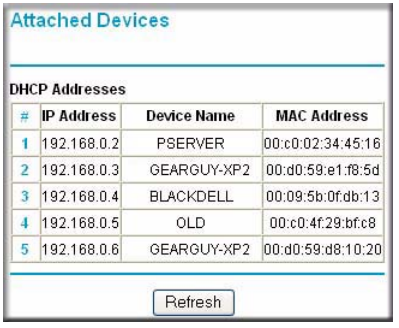


Figure 4-6

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the modem router is rebooted, the table data is lost until the modem router rediscovers the devices. To force the modem router to look for attached devices, click the **Refresh** button.

Viewing, Selecting, and Saving Logged Information

The modem router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown in the following figure:

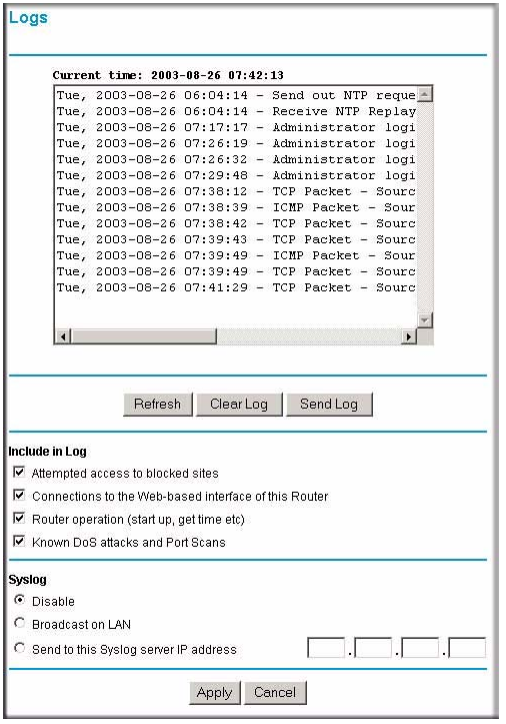

Logs
Current time: 2003-08-26 07:42:13
Tue, 2003-08-26 06:04:14 - Send out NTP reque
Tue, 2003-08-26 06:04:14 - Receive NTP Replay
Tue, 2003-08-26 07:17:17 - Administrator logi
Tue, 2003-08-26 07:26:19 - Administrator logi
Tue, 2003-08-26 07:26:32 - Administrator logi
Tue, 2003-08-26 07:29:48 - Administrator logi
Tue, 2003-08-26 07:38:12 - TCP Packet - Sourc
Tue, 2003-08-26 07:38:39 - ICMP Packet - Sour
Tue, 2003-08-26 07:38:42 - TCP Packet - Sourc
Tue, 2003-08-26 07:39:43 - TCP Packet - Sourc
Tue, 2003-08-26 07:39:49 - ICMP Packet - Sour
Tue, 2003-08-26 07:39:49 - TCP Packet - Sourc
Tue, 2003-08-26 07:41:29 - TCP Packet - Sourc
Refresh
Clear Log
Send Log
Include in Log
Attempted access to blocked sites
Connections to the Web-based interface of this Router
Router operation (start up, get time etc)
Known DoS attacks and Port Scans
Syslog
Disable
Broadcast on LAN
Send to this Syslog server IP address
Apply
Cancel

Figure 4-7

Log entries are described in the following table.

Table 4-4. Security Log Entry Descriptions

Field	Description
Current time	The date and time the log entry was recorded.
Description or action	The type of event and what action was taken if any.

Table 4-4. Security Log Entry Descriptions

Field	Description
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it is on the LAN or WAN.

Log action buttons are described in the following table.

Table 4-5. Log Action Buttons

Field	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.
Apply	Apply the current settings.
Cancel	Clear the current settings.

Selecting Which Information to Log

Besides the standard information listed previously, you can choose to log additional information. Those optional selections are as follows:

- Attempted access to blocked site
- Connections to the Web-based interface of the modem router
- Modem Router operation (start up, get time, etc.)
- Known DoS attacks and port scans

Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select to the **Broadcast on LAN** radio button or enter the IP address of the server where the syslog file will be written.

Log Message Examples

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second.

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:10.0.0.3
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:10.0.0.3
```

[This entry shows an administrator logging in and out from IP address 10.0.0.3.]

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:10.0.0.3
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was e-mailed.]

Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

[These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

To receive logs and alerts by e-mail, you must provide your e-mail information in the E-mail screen:

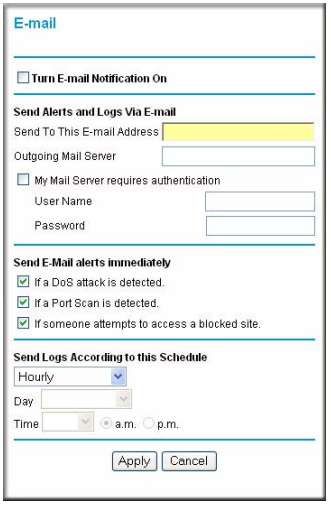
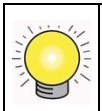


Figure 4-8

- **Turn e-mail notification on**. Select this check box if you want to receive e-mail logs and alerts from the modem router.
- **Send alerts and logs via email**.
  - **Send To This E-mail Address.** Enter the e-mail address where you want to send the alerts and logs. Use a full e-mail address, such as ChrisXY@myISP.com.
  - **Outgoing Mail Server**. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
  - **My Mail Server requires authentication**. Select this check box if you need to log in to your SMTP server to send E-mail. If you select this feature, you must enter the user name and password for the mail server.



Tip: If you cannot remember this information, check the settings in your e-mail program.

- **Send alert immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - **Day for sending log**. Specifies which day of the week to send the log. Relevant when the log is sent weekly.
  - **Time for sending log**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the **Weekly**, **Daily**, or **Hourly** option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

Running Diagnostic Utilities and Rebooting the Modem Router

The modem router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the modem router:

- Ping an IP address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the routing table to identify what other modem routers the modem router is communicating with.
- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

From the main menu, under the Maintenance heading, select Modem Router Diagnostics to display the Diagnostics screen:

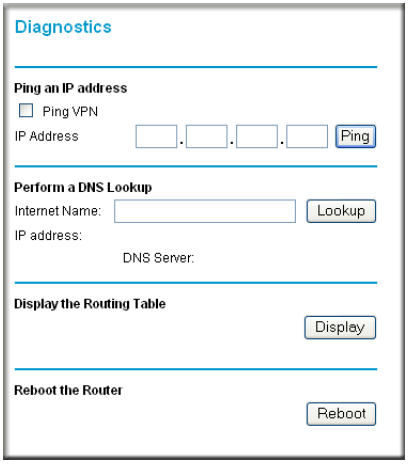


Figure 4-9

Enabling Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your modem router.

Tip: Be sure to change the modem router default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper-case and lower-case), numbers, and symbols. Your password can be up to 30 characters.

Configuring Remote Management

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.

2. Under the Advanced heading of the main menu, select Remote Management to display the Remote Management screen:

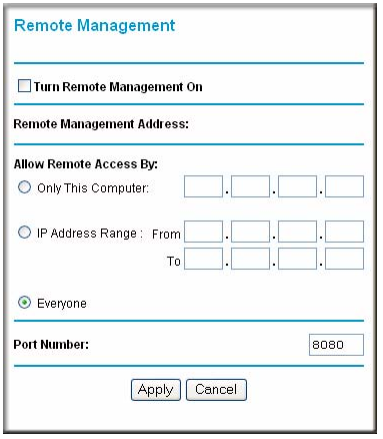


Figure 4-10

3. Select the **Turn Remote Management On** check box.
4. Specify which external addresses will be allowed to access the modem router's remote management.

   For security, restrict access to as few external IP addresses as practical:

   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.

5. Specify the port number that will be used for accessing the management interface.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the field provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

6. Click **Apply** to have your changes take effect.

When accessing your modem router from the Internet, you will type your modem router WAN IP address in your Internet browser address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter:

http://134.177.0.123:8080

	Note: In this case, you must include http:// in the address.

Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your ADSL2+ Modem Wireless Router.

The ADSL2+ Modem Wireless Router provides a variety of advanced features, such as the following:

- "Modifying Your WAN Setup"
- "Configuring Your LAN IP Settings"
- "Using the Modem Router as a DHCP Server"
- "Configuring Dynamic DNS"
- "Using Static Routes"
- "Configuring Universal Plug and Play (UPnP)"
- "Configuring Wireless Bridging and Repeating (WDS)"

These features are discussed in the following sections of this chapter.

Modifying Your WAN Setup

To view or change the WAN Setup:

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** and default password of **admin**, or using whatever password and LAN address you have chosen for the modem router.

2. From the main menu, select WAN Setup to display the WAN Setup screen:

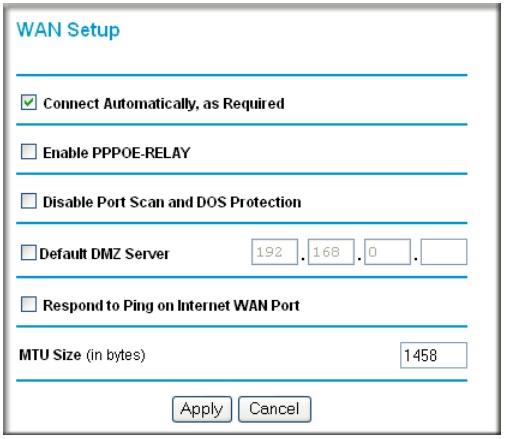


Figure 5-1

3. Make the changes that you want, and then click **Apply** to save the settings.

The WAN Setup fields are described in the following table:

Table 5-1. WAN Setup Settings

Setting	Description
Connect Automatically, as Required	Usually, this check box is selected, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting. • If disabled, you must connect manually, using the screen accessed from the **Connection Status** button on the Router Status screen. • If you have an "Always on" connection, this setting has no effect.
Enable PPPOE-RELAY	If this check box is selected, this feature allows a PPPoE client on a local PC to a remote PPPoE server with the gateway acting as a relay agent.
Disable Port Scan and DOS Protection	This check box is usually clear so that the firewall protects your LAN against port scans and denial of service (DOS) attacks. This check box should be selected only in special circumstances.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See "Setting Up a Default DMZ Server" on page 5-3.

Table 5-1. WAN Setup Settings

Setting	Description
Respond to Ping on Internet WAN Port	If you want the modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Setting Up a Default DMZ Server

Warning: For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with NAT. The modem router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

Incoming traffic from the Internet is normally discarded by the modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

To assign a computer or server to be a default DMZ server:

1. Go to the WAN Setup screen as described in the previous section.
2. Select the **Default DMZ Server** check box.
3. Type the IP address for that server.
4. Click **Apply** to save your changes.

Configuring Your LAN IP Settings

The LAN IP Setup screen allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the modem router main menu.

The modem router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The modem router default LAN IP configuration is:

- LAN IP addresses: 10.0.0.2
- Subnet mask: 255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this screen.

To view or change the LAN IP Setup:.

	Warning: If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected and so will others connected to the modem router. To connect to the modem router, you must open a new connection to the new IP address and log in again. Others using the modem router must restart their computers to connect to the modem router again.

1. Select LAN IP to display the LAN IP Setup screen:

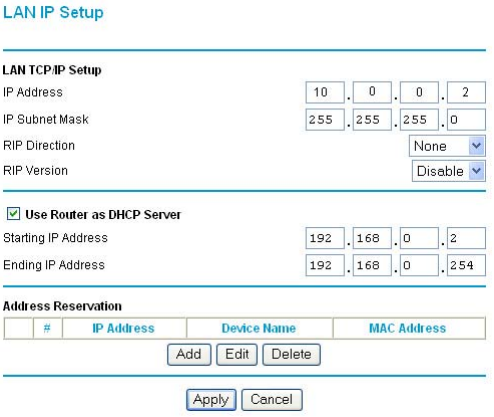


Figure 5-2

2. Change the settings. For more information, see Table 5-2, "Using the Modem Router as a DHCP Server" on page 5-6 or "Defining Reserved IP Addresses" on page 5-7.
3. Click **Apply** to save the changes.

The LAN TCP/IP Setup parameters are explained in the following table.

Table 5-2. LAN IP Setup

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the modem router.
	IP Subnet Mask	The LAN subnet mask of the modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.
	RIP Direction	RIP (Router Information Protocol) allows a modem router to exchange routing information with other routers. This setting controls how the modem router sends and receives RIP packets. **Both** is the default. • **Both** or **Out Only**. The modem router broadcasts its routing table periodically. • **Both** or **In Only**. The modem router incorporates the RIP information that it receives. • **None**. The modem router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, this is **RIP-1**. • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information, see "Using the Modem Router as a DHCP Server" on page 5-6.	Use Router as a DHCP Server	This check box is usually selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. See "Using the Modem Router as a DHCP Server" on page 5-6.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

Table 5-2. LAN IP Setup

Settings	Description
Address Reservation For more information, see "Using the Modem Router as a DHCP Server" on page 5-6.	When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Using the Modem Router as a DHCP Server

By default, the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem router's LAN. The assigned default gateway address is the LAN address of the modem router. IP addresses is assigned to the attached PCs from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the modem router are satisfactory. See the online document listed in "Internet Networking and TCP/IP Addressing" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP Server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box on the LAN IP Setup screen. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by filling in the **Starting IP Address** and **Ending IP Address** fields. These addresses should be part of the same IP address subnet as the modem router's LAN IP address. Using the default addressing scheme, you should define a range between 10.0.0.3 and 10.0.0.254, although you might want to save part of the range for devices with fixed addresses.

The modem router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined.
- Subnet mask.
- Gateway IP Address is the router's LAN IP address.
- Primary DNS server, if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address.
- Secondary DNS server, if you entered a secondary DNS address in the Basic Settings screen.

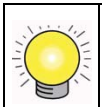
- WINS Server (Windows Internet Naming Service Server), determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Defining Reserved IP Addresses

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it access the modem router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the **Add** button.
2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 10.0.0.x.
3. Type the MAC address of the computer or server.



Tip: If the computer is on your network, it is listed on the same page for your convenience. Clicking the radio button for each entry in the attached device list fills in the fields automatically with the computer's MAC address and name.

4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service to register your domain to their IP address, and forward traffic directed at your domain to your frequently changing IP address.

The modem router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the modem router, whenever your ISP-assigned IP address changes, your modem router will automatically contact your Dynamic DNS service provider, log in to your account, and register your new IP address.

To configure Dynamic DNS:

	Warning: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses will not be routed on the Internet.

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.
2. From the main menu, select Dynamic DNS to display the Dynamic DNS screen:

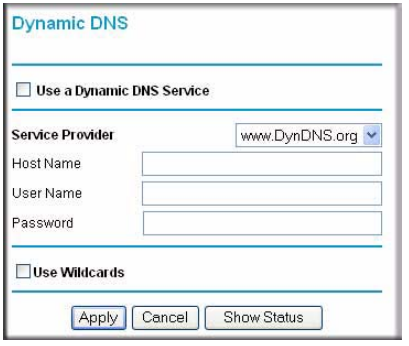


Figure 5-3

3. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, and register for an account.

For example, for dyndns.org, go to www.dyndns.org.

4. Select the **Use a Dynamic DNS Service** check box.
5. Select the name of your dynamic DNS service provider.
6. Fill in the **Host Name**, **User Name**, and **Password** fields.

   The dynamic DNS service provider may call the host name a domain name. If your URL is myName.dyndns.org, then your host name is myName. The password can be a key for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature.

   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Using Static Routes

Static routes provide additional routing information to your modem router. Under normal circumstances, the modem router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 10.0.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the modem router, and a second static route was created to your local network for all 10.0.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 10.0.0.100. The static route would look like Figure 5-5.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** fields specify that all traffic for these addresses should be forwarded to the ISDN router at 10.0.0.100.
- In the **Metric** field, a value of 1 will work since the ISDN router is on the LAN. This represents the number of routers between your network and the destination. This is a direct connection, so it is set to 1.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

Configuring Static Routes

1. Log in to the modem router at its default LAN address of **http://10.0.0.2** with its default user name of **admin** and default password of **admin**, or using whatever user name, password and LAN address you have chosen for the modem router.
2. From the main menu, under the Advanced heading, select Static Routes to view the Static Routes screen:

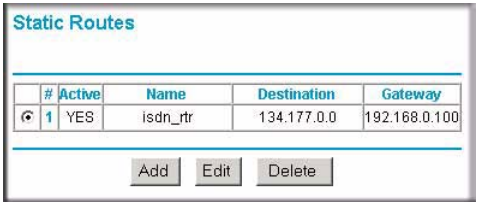


Figure 5-4

3. Click **Add** or **Edit** to display the following screen:

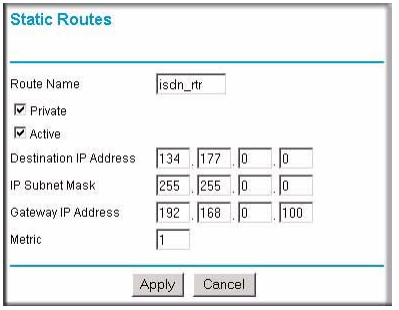


Figure 5-5

4. Fill in or change the fields:
   - **Route Name.** The route name is for identification purposes only.
   - **Private**. Select this check box if you want to limit access to the LAN only. The static route will not be reported in RIP.
   - **Active**. Select this check box to make this route effective.
   - **Destination IP Address**, and **IP Subnet Mask**. If the destination is a single host, type a subnet value of **255.255.255.255**.
   - **Gateway IP Address**. This must be a router on the same LAN segment as the modem router.
   - **Metric**. Type a number between 2 and 15. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 2.
5. Click **Apply** to either save your changes. If you added a static route, it is added to the Static Routes screen.

Configuring Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Select UPnP on the main menu to display the UPnP screen:

Figure 5-6

2. Fill in the settings on the UPnP screen:

   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the modem router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.
   - **Advertisement Period**. The advertisement period is how often the modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal and external) that device has opened.

3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the modem router.
   - Click **Cancel** to disregard any unsaved changes.

- Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Configuring Wireless Bridging and Repeating (WDS)

You can build large bridged wireless networks by using the modem router to configure a wireless distribution system (WDS). On the main menu, below the Advanced heading, select Wireless Settings, and then select the **WDS** radio button. The following screen displays:

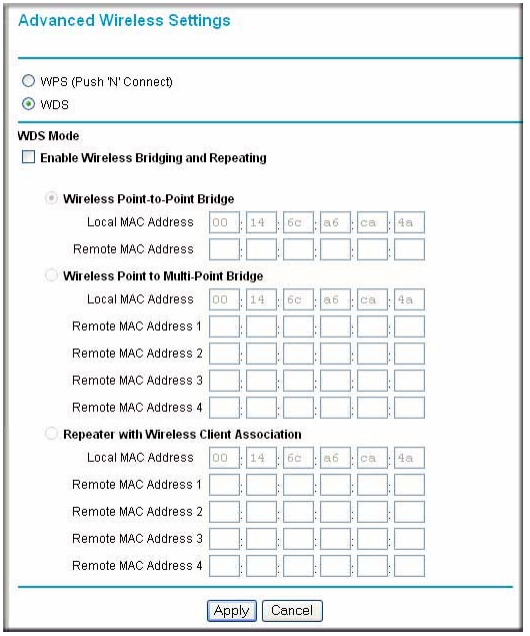


Figure 5-7

	Note: Unless you change the security configuration, the wireless bridging and repeating feature uses the default security profile to send and receive traffic.

Here are some examples of wireless bridged configurations:

- **Point-to-Point bridge**. The modem router communicates with another bridge-mode wireless station. See "Point-to-Point Bridge Configuration".

- **Multi-Point bridge**. The modem router is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this “master,” rather than to other access points. See “Multi-Point Bridge Configuration”.
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See “Repeater with Wireless Client Association”.

Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the DG834GUv5 modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled—only wired clients can be connected. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication.

The following figure shows an example of Point-to-Point Bridge mode.

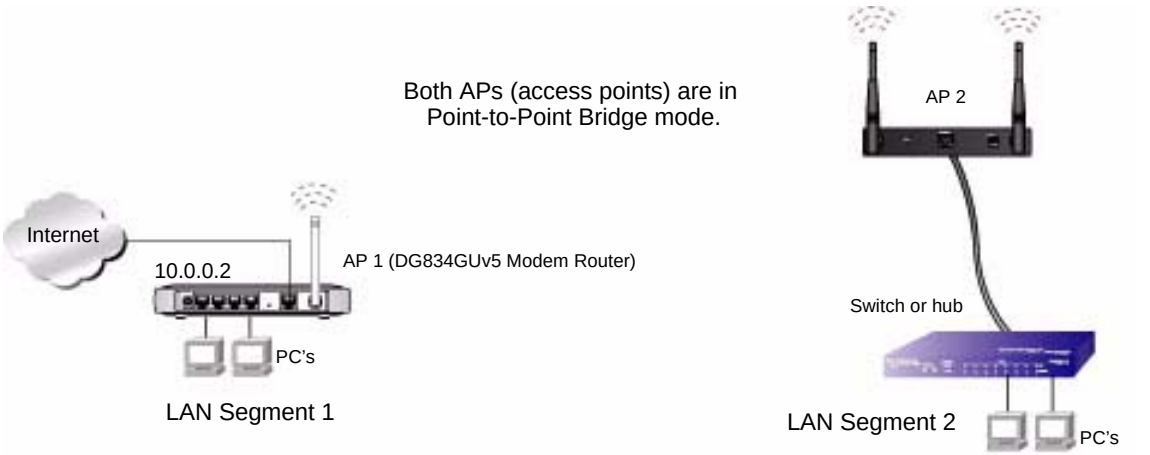


Figure 5-8

To set up a point-to-point bridge configuration (shown in Figure 5-8):

1. Configure the DG834GUv5 modem router (AP 1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the other access point (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode.

   The DG834GUv5 modem router must have AP 2’s MAC address in its **Remote MAC Address** field, and AP 2 must have the DG834GUv5’s MAC address in its **Remote MAC Address** field.
3. Configure and verify the following for both access points:

- Both APs must use the same SSID, channel, authentication mode, if any, and security settings if security is in use.

4. Disable the DHCP server on AP2. AP1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Multi-Point Bridge Configuration

Multi-Point Bridge mode allows a modem router to bridge to multiple peer access points simultaneously. As a bridge, wireless client associations are disabled—only wired clients can be connected. Multi-Point Bridge mode configuration includes the following steps:

- Entering the MAC addresses of the other access points in the fields provided.
- Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this DG834GUv5 as the Remote MAC Address.
- Using wireless security to protect this traffic.

The figure below shows an example of a Multi-Point Bridge mode configuration.

The DG834GUv5 is AP 1, which is the "Master AP" in Point-to-Multi-Point Bridge mode.

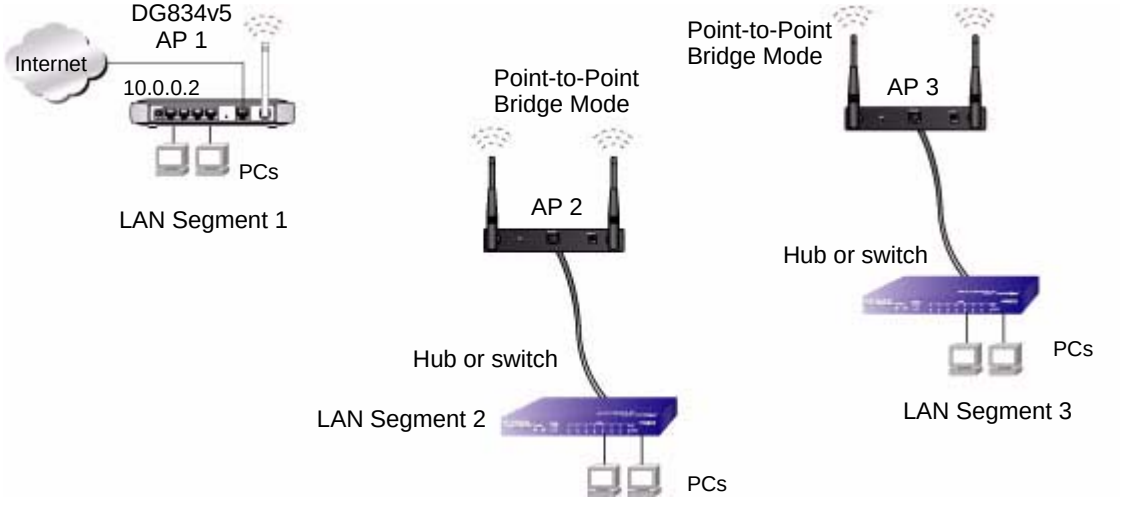


Figure 5-9

To set up the multi-point bridge configuration shown in Figure 5-9:

1. Configure the operating mode of the modem routers.
   - Because it is in a central location, configure the DG834GUv5 modem router (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode and enter the MAC addresses of AP 2 and AP 3 in the **Remote MAC Address 1** and **Remote MAC Address 2** fields.
   - Configure the access point (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the remote MAC address of the DG834GUv5 modem router.
   - Configure the access point (AP3) on LAN Segment 3 in Point-to-Point Bridge mode with the remote MAC address of the DG834GUv5 modem router.
2. Disable the DHCP server on AP2 and AP3. AP1 will then be the DHCP server.
3. Verify the following for all access points:
   - The LAN network configuration of the modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.
   - Only one AP, the DG834GUv5 modem router in Figure 5-9, is configured in Point-to-Multi-Point Bridge mode; all the others are in Point-to-Point Bridge mode.
   - All APs, including the DG834GUv5 modem router, must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.
   - All APs, including the DG834GUv5 modem router, must use the same SSID, channel, authentication mode, if any, and encryption in use.
   - All point-to-point APs must have the MAC address of AP 1 (the DG834GUv5 modem router in the above diagram) in the **Remote AP MAC address** field.
4. Verify connectivity across the LANs.
   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

	Note: Wireless stations configured as they are in Figure 5-9 will not be able to connect to the modem router or access points. If you require wireless stations to access any LAN segment, you can use additional access points configured in Wireless Access Point mode in any LAN segment.

Repeater with Wireless Client Association

In this mode, the ADSL2+ Modem Wireless Router sends all traffic to a remote AP. For Repeater mode, you must enter the MAC address of the remote “parent” access point. Alternatively, you can configure the ADSL2+ Modem Wireless Router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this ADSL2+ Modem Wireless Router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the DG834GUv5 is the parent AP it can connect with up to four child APs.

The following figure shows an example of a Repeater Mode configuration.

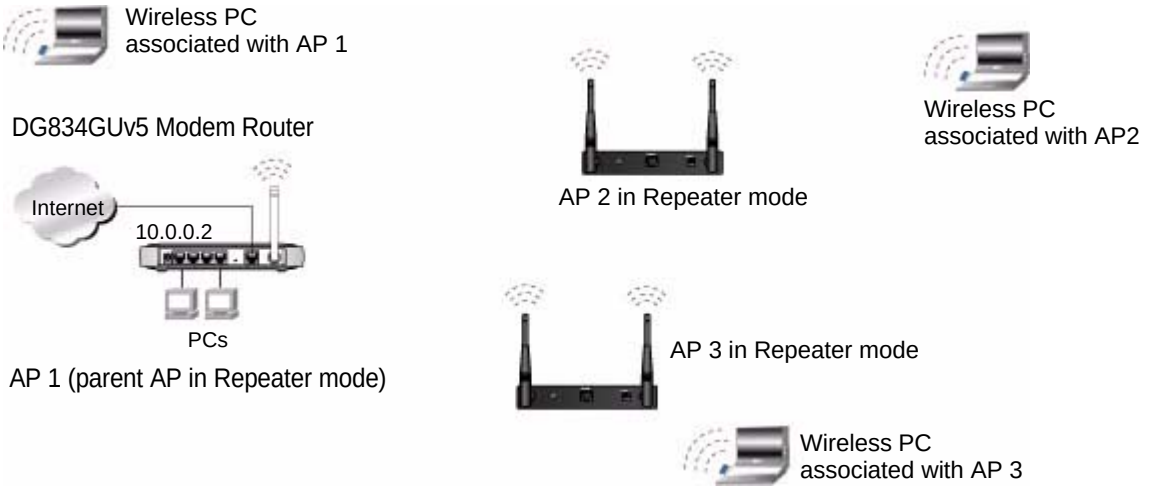


Figure 5-10

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
   - Configure AP 1 the DG834GUv5 modem router in the previous figure) on LAN Segment 1 with the MAC address of AP 2 and AP 3 in the first two **Remote MAC Address** fields.
   - Configure AP 2 with the MAC address of AP 1 in the **Remote MAC Address** field.
   - Configure AP 3 with the MAC address of AP 1 in the **Remote MAC Address** field.
2. Verify the following for both access points:

- The APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same subnet.
- AP devices must use the same SSID, channel, authentication mode, and encryption.

3. Disable the DHCP servers on repeaters AP2 and AP3. AP1 will then be the DHCP server.

4. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

Chapter 6
Configuring Telkom VPN Lite

This chapter describes how to configure your DG834GUv5 Wireless Router to work with the Telkom VPN Lite service.

What is VPN Lite?

A world first in Do-It-Yourself networking. After ordering VPN Lite, Telkom provides you with secure access to a web portal which is used to create all the sites and individual connections needed for your own secure Virtual Private Network (VPN). As your business needs change you can adapt the network size as well as your usage bundle up or down when required. You are therefore not tied into a contract which is not ideal for your business at any given time. It is the lowest cost and easiest to use networking solution in a box on offer today.

It allows you to communicate between branches, between businesses and even between individuals. You can connect up to 50 sites on a VPN Lite network without affecting you monthly bill. VPN Lite offers a discounted bundle of your choice which it is not capped. Private static IP addresses allows for any site to communicate with any other site on the network.

Note: For more information about the Telkom VPN Lite service offering, please visit: http://www.telkom.co.za/products_services/vpnlite/index.html

Configuring VPN Lite

The VPN Lite Setup Wizard included in the GUI confiruation tool of the DG834GUv5 was developed to assist users to easily configure VPN Lite network connections.

To start the VPN Lite Wizard, login to your ADSL2+ Modem Wireless Router:

1. Type **http://routerlogin.net** or **http://10.0.0.2** in the address field of an Internet browser.

Figure 6-1

This login window opens:

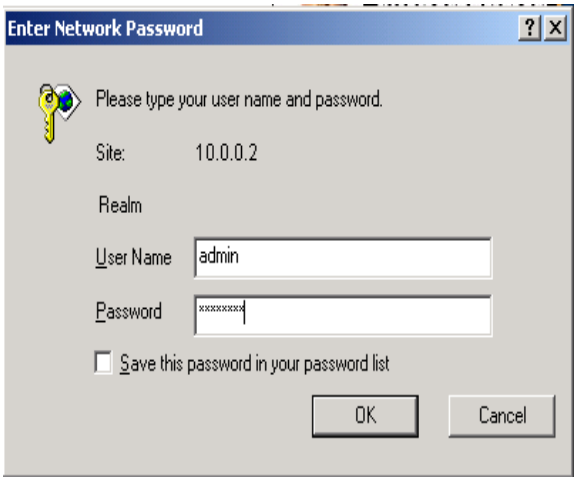


Figure 6-2

2. Enter **admin** for the user name and **admin** for the password, both in lower case letters.
3. Click **OK.** You will be logged in to your router's main menu.
4. Selet to **VPN Lite Wizard** option from the left hand navigation panel of the router's main menu:

Figure 6-3

5. After reading the notice on the VPN Lite setup page, click Next to continue.
6. Input the VPN Lite username and password that was configured on the Telkom VPN Lite Webpage:

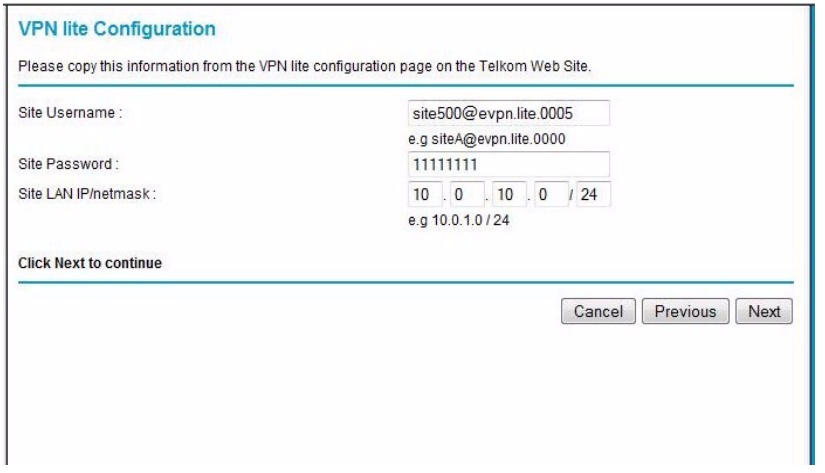


Figure 6-4

7. The LAN IP address and Subnet mask that was configured on the Telkom VPN Lite Website must also be entered.

	Note: The IP address for each site configured must be different and fall within a different IP Subnet range.Example: site1@evpn.lite.0001 can be 10.0.1.0/24, then the IP subnet for site2@evpn.lite.0002 must be a different subnet, like 10.0.2.0/24. The IP Address must correspond exactly to the one configured on theVPN Lite Webpage.

8. Review the configuration details you have entered and click **Finish** if you are satisfied to complete the VPN Lite setup:

VPN Lite Site Confirmation
Your router will be setup with the following details.
Site Username :
site500@evpn.lite.0005
Site Password :
11111111
Site LAN IP/netmask :
10.0.10.0/24
NEW Router IP :
10.0.10.2
Click FINISH to complete your VPN lite setup
(After clicking FINISH, you will need to use the NEW router IP to connect to your router. Please wait until the progress bar has completed before reconnecting)
Cancel
Previous
Finish

Figure 6-5

	Note: After selecting Finish, you may need to connect to your router with the new LAN IP address entered during configuring VPN Lite. Please wait until the progress bar on the router menu page has completed before attempting to reconnect.

Chapter 7
Troubleshooting

This chapter gives information about troubleshooting your ADSL2+ Modem Wireless Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?

  Go to "Basic Functioning" on page 7-1.
- I can't access the router's configuration with my browser.

  Go to "Troubleshooting Access to the Modem Router Main Menu" on page 7-2.
- I've configured the router but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 7-3.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 7-8.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify that:
   a. The Power LED is still solid green. A red light indicates the unit has failed its power-on self-test (POST).
   b. The Ethernet LAN port LEDs are lit for any local ports that are connected.

      If a LAN port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.
   c. The DSL and Internet LEDs are lit.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Is Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

Power LED Is Red

When the router is turned on, the modem router performs a power-on self-test. If the Power LED turns red, there is a fault within the router. Try to clear the fault as follows:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This sets the router's IP address to 10.0.0.2. This procedure is explained in "Restoring the Default Configuration and Password" on page 7-8.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or DSL or Internet Port LEDs Are Not On

If these LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure that you are using the correct cable. When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834GUv5.

Troubleshooting Access to the Modem Router Main Menu

If you are unable to access the modem router main menu from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.

- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 10.0.0..3 to 10.0.0.254. See the online document listed in "Preparing a Computer for Network Access" in Appendix B to find your computer's IP address.

> **Note:** If your computer's IP address is shown as 169.254.x.x:
> Recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 10.0.0.2. This procedure is explained in "Restoring the Default Configuration and Password" on page 7-8.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **admin**. Make sure that Caps Lock is off when entering this information.

If the router does not save changes you have made in the Web configuration interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Troubleshooting the ISP Connection

ADSL Link

If your router is unable to access the Internet, you should first determine whether you have a DSL link with the service provider. The state of this connection is indicated with the DSL LED.

ADSL Link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the DSL LED.

DSL LED Is Solid Green

If your DSL LED is solid green then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

DSL LED Is Blinking

If your DSL LED is blinking, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn solid green within a few minutes.

If the DSL LED does not turn solid green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a solid green DSL LED, there may be a problem with your wiring. If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

DSL LED Is Off

If the DSL LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a solid green DSL LED the problem may be one of the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Obtaining a WAN IP Address

If your modem router is unable to access the Internet, and your Internet LED is green or blinking green, determine whether the modem router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser, and select an external site such as www.netgear.com.
2. Access the modem router main menu at **http://10.0.0.2**.
3. Under the Maintenance heading, check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a multiplexing method or virtual path identifier or virtual channel identifier parameter.
  Verify with your ISP the multiplexing method and parameter value, and update the router's ADSL settings accordingly.
- Your ISP might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.
- If you have selected a login program, the service name, user name, and password might be set incorrectly. See "Troubleshooting PPPoE or PPPoA", below.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case try either of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at **http://10.0.0.2**.
2. Under the Maintenance heading, select Router Status.
3. Click **Connection Status**.
4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, the service name, user name, or password might be incorrect. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your modem router can obtain an IP address but your computer is unable to load any Web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer and verify the DNS address as described in "Preparing a Computer for Network Access" in Appendix B . Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address as described in the link to the online document "Preparing a Computer for Network Access" in Appendix B .

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your PC to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   `ping 10.0.0.2`
3. Click **OK**.

   You should see a message like this one:

   `Pinging <IP address> with 32 bytes of data`

   If the path is working, you see this message:

   `Reply from < IP address >: bytes=32 time=NN ms TTL=xxx`

   If the path is not working, you see this message:

   `Request timed out`

   If the path is not working correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in "LAN or DSL or Internet Port LEDs Are Not On" on page 7-2.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device.

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type:

   `PING -n 10` *IP address*

   where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default modem router as described in the online document listed in "Preparing a Computer for Network Access" in Appendix B .
- Make sure that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to clone or spoof the MAC address from the authorized PC. See the *Wireless ADSL2+ Modem Router Setup Manual*.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password toadmin and the IP address to **10.0.0.2**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function (see "Backing Up, Restoring, or Erasing Your Settings" on page 4-1).

- Press both the Wireless button and WPS button on the side of the modem router for 5 seconds. Use this method for cases when the administration password or IP address is not known.

	Note: Pressing the reset button on the modem router reboots the unit but does not restore the factory default settings.

Problems with Date and Time

The E-mail screen in the Content Filtering section displays the current date and time of day. The ADSL2+ Modem Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
  Cause: The router does not automatically sense daylight savings time. On the E-mail screen, select or clear the **Adjust for Daylight Savings Time** check box.

Chapter 8
Connecting a USB Drive to the Router

This chapter describes how to configure a USB disk drive attached to the DG834GUv5 Wireless Router. In planning your network, you should consider the level of security required for local and remote users of the USB drive.
You can connect either a USB flash drive or a USB hard drive to the DG834GUv5. USB drive applications may include:

- Sharing files with offsite coworkers — sharing files such as Word documents, PowerPoint presentations, and text files with remote users.
- Sharing multimedia with friends and family — sharing MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network — storing files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between the systems.

Note: As soon as you plug the USB drive in the router, local users have read and write access to the drive using Microsoft Networking.
Users from the Internet can access the USB drive using FTP. The USB Drive Wizard will guide you through the FTP setup process.

File Sharing Scenarios

You need to prepare the following before you can set up your Product Family:

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any PC, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia.
A few of the common uses are shown below.

Sharing Photos with Friends and Family

The DG834GUv5 allows you to create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo sharing site.

Sharing Photos With Friends and Family

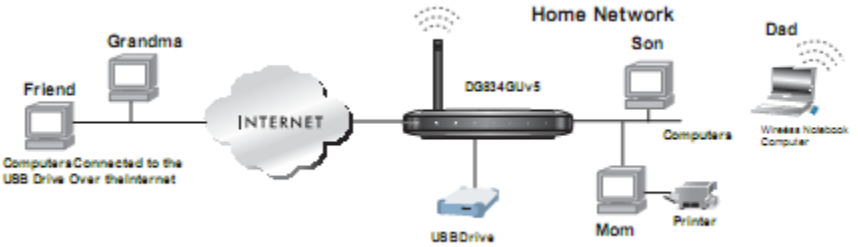


Figure 8-1: Sharing photos with friends and family

Sharing files with your friends and family involves the following steps:

1. Using the DG834GUv5 Wireless Router configuration utility, assign a username and password for each friend or family member.
2. Specify a share folder that the account can access.
3. Decide whether the account should have read only or read and write privileges. You can assign read only access of the shared folder on the USB drive to remote friends and family members such as Grandma.
4. Local family members (Mom, Dad, and Son) can use a Web browser or Microsoft Networking to access files on the USB drive. Local users have read and write privilege

For more information on sharing photos with friends and family who are at another location, see “Connecting to the USB Drive from a Remote Computer” on page 8-11.

For more information on sharing photos with family on your local network, see “Connecting to the USB Drive from a Local Web Browser” on page 8-11 and “Connecting to the USB Drive From Your Home/Office Network” on page 8-12.

Storing Files in a Central Location for Playing or Printing

The DG834GUv5 Wireless Router enables you to move files so that a private resource can act as a network resource. The DG834GUv5 allows centralized storage for easy access from other computers that have local printers, CD burners, speakers, or specialized software.
For example, the following scenario may occur in a typical family that has one high quality color printer directly attached to a computer, but not shared on the LAN:

- The daughter has some photos on her Macintosh computer that she wants to print.
- The mother has a photo-capable color printer directly attached to her PC, but not shared on the network.
- The mother and daughter's computers are not visible to each other on the network

Storing Files in a Central Location

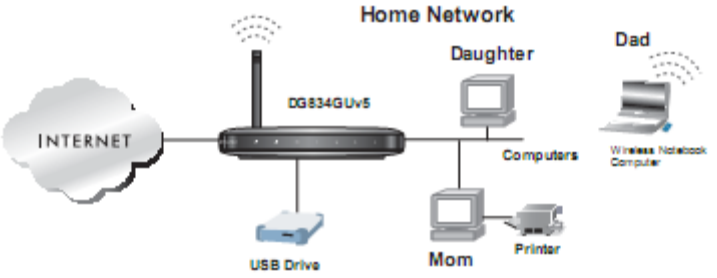


Figure 8-2: Storing files in a central location for printing

How can you send the photos from the daughter's Mac to a printer attached to the mother's PC? This is where the USB drive on the Wireless Router can save you time and effort.

1. Copy the photos from the daughter's Mac to the USB drive using a Web browser. See "Connecting to the USB Drive from a Local Web Browser" on page 8-11 for more information.
2. Use the mother's PC to retrieve the files for printing. You can use a Web browser or Microsoft Networking to transfer the files from the USB drive to a PC. For more information on using Microsoft Networking to transfer the files, see "Connecting to the USB Drive From Your Home/Office Network" on page 8-12.

Sharing Large Files with Colleagues

Sending files that are larger than 5 MB can pose a problem for many mail systems. The DG834GUv5 Wireless Router allows you to share very large files such as PowerPoint presentations or ZIP files with colleagues at another site. Rather than tying up their mail systems will large files, your colleagues can use FTP to easily download shared files from the DG834GUv5.

Sharing Large Files With Colleagues

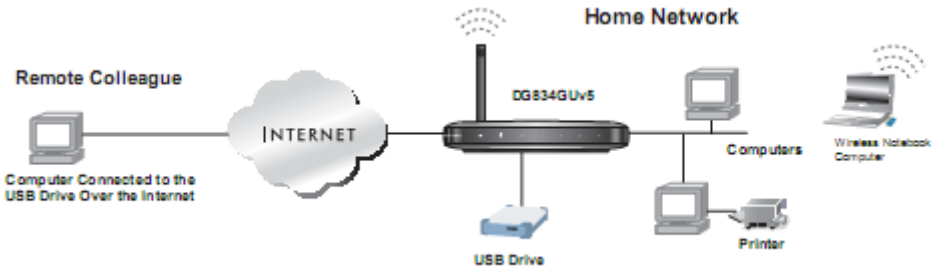


Figure 8-3: Sharing files with remote users

Sharing files with a remote colleague involves the following steps:

1. Using the DG834GUv5 Wireless Router configuration utility, assign a username and password for your colleague.
2. Specify a share folder on the USB drive that the colleague can access.
3. The remote colleague can use FTP from a Web browser or another FTP program to access the shared folder on the USB drive. Access can be read only or read/write for remote users.

For more information, see “Connecting to the USB Drive from a Remote Computer” on page 8-11.

Understanding the USB Configuration Settings

To configure the USB disk drive settings, click the USB Drive Settings link in the main menu of the browser interface. The USB Drive Settings screen appears, as shown below.

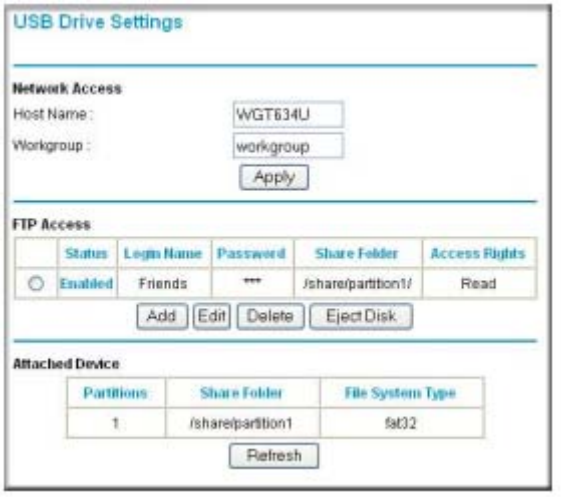


Figure 8-4: USB Drive Settings screen

The USB Drive Settings screen shows which login accounts are enabled and the share folders each account has access to. The following fields are displayed:

Network Access

- **Host Name**. The host name you can use to access the USB drive from your network.
- **Workgroup**. If you are using a Windows Workgroup rather than a Domain, the Workgroup name will be displayed here.

FTP Access

- **Status.** Access is enabled or disabled for the login account listed.
- **Login Name**. The user who has rights to access the USB disk drive.
- **Password**. For security purposes, the password for each login account is not displayed.
- **Share Folder**. The top directory of the USB drive the login account has access to.
- **Access Rights**. Read Only or Read & Write access to the top directory designated as the share, and all directories below the share.

Attached Device

- **Partitions**. The partition number on the USB drive.
- **Share Folder**. The top or root directory of the USB drive.
- **File System Type**. The file system on the partition can be FAT, FAT32, NTFS (read only), or Linux.

Connecting a USB Drive to the DG834GUv5

	Note: Unlike local network data, your router's USB drive can be accessed beyond your network by anyone with the proper credentials. This is especially true for the wireless network in your home. For this reason, use the security features of your router.

The DG834GUv5 Wireless Router provides highly effective security features which are covered in detail in Chapter 2, "Wireless Configuration" and Chapter 5, "Advanced Configuration". Deploy the security features appropriate to your needs.

The USB port of the DG834GUv5 is a standard USB connector.

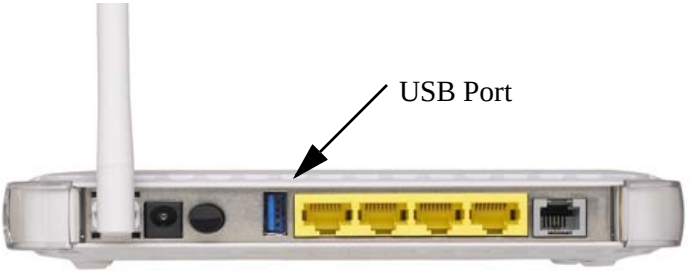


Figure 8-5: Router USB Port

You can connect a USB drive to the DG834GUv5 Wireless Router in the following ways:

- Connect a USB "flash drive", also known as a "flash memory stick", directly to the port.
- Connect an external USB disk drive using a standard USB cable.

USB Drive Requirements

The DG834GUv5 Wireless Router conforms to the USB 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown below.

Table 5-1. USB Bus Speeds

Bus Name	Speed/Second
USB 1.1	12 Mbits
USB 2.0	480 Mbits

Actual bus speeds will vary, depending on the CPU speed, memory, speed of the network, and other variables.

The DG834GUv5 should work with all USB-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the DG834GUv5 Router, go to:

http://kbserver.netgear.com/kb_web_files/n101300.asp

The USB port on the DG834GUv5 can only be used to connect USB storage class devices like hard drives. USB modems, printers, CD ROM drives, and DVD drives cannot be connected to the device.

Note: The USB port on the DG834GUv5 can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.

The DG834GUv5 supports FAT, FAT32, NTFS (read only) and Linux file systems. As soon as a USB hard disk or flash memory is attached to DG834GUv5 USB port, users on the local area network can access the USB drive with full read and write access.

Using the USB Drive Setup Wizard to Allow Remote Access from the Internet

You can use the USB Drive Wizard to quickly and easily share directories on the USB drive after you have attached it to the router.

1. Log in to the DG834GUv5 router at its default LAN address of *http://10.0.0.2* with its default user name of **admin** and default password of **admin**, or using whatever LAN address and password you have set up

2. Select **USB Drive Wizard** in the left navigator to display the screen shown below:

Figure 8-6: Select the folder to share

3. Type the folder name to share. To share the whole USB drive, type \. To share a specific folder on the USB drive, type

\<my folder> where <my folder> is replaced with the name of your folder. All files and subfolders below \ or \<my folder> will be accessible. Click Continue.

4. Type the user login name you want to give FTP access to the drive:

Figure 8-7: Type the user login name

Click Continue.

5. Type the password the user will use for FTP access.
6. Select the FTP access rights:

Users can have either Read Only or Read & Write access.

Figure 8-8: Select Read Only or Read & Write

7. Click Continue to view the list of shared folders.

Click Finish

Using the USB Drive Menu to Grant FTP Access Rights

You can also use the USB Drive menu to share directories on the USB drive after you have attached it to the router.

Granting Users Access to the USB Drive

To give a login account access to the USB disk drive:

1. Select the USB Drive Settings link in the left navigator.
2. Click **Add** to view the screen shown below.

Figure 8-9: Granting an account access to the USB Device

3. Select **Enabled** to give access to the USB drive.
4. Type the login account name that you want to give access to the USB drive.
5. Type the password for the account and repeat it.
6. For the Share Folder, type the name of the USB drive's top directory you want the account to have access to.
7. Select the access rights to give to the root directory and all directories below it — Read Only or Read & Write.
8. Click **OK** to save your settings.

Unmounting a USB Drive

To unmount a USB disk drive so that no users can access it, from the USB Drive Settings screen, click the Eject Disk button. This takes the drive offline.

Note: You should unmount the USB drive first before physically unplugging it from the router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it may result in file or disk corruption.

Understanding the USB Drive Access Methods

There are three ways you can allow users to connect to the USB drive:

1. Local Web browser — users on the local area network can use the USB drive's local IP address from a Web browser. LAN access rights are read/write unless you restrict access on a file or directory basis. See "Connecting to the USB Drive from a Local Web Browser" on page 8-11.
2. Remote Web browser — users outside your local network can access files on the USB drive from a Web browser at its WAN IP address. WAN access is by FTP and is read only or read/write according to the user access rights you set. See "Connecting to the USB Drive from a Remote Computer" on page 8-11.
3. Microsoft Network access — allows users on the local area network to access files on the USB drive from Windows Explorer. Windows Explorer rights are read/write unless you restrict access on a file or directory basis. See "Connecting to the USB Drive From Your Home/Office Network" on page 8-12.

Connecting to the USB Drive from a Local Web Browser

You can connect to the USB drive from local computers using a Web browser.

1. Type \\ followed by the router's IP address:

\\10.0.0.2

2. Type the account name and password that has access rights to the USB drive.
3. The root directories of the USB drive that the login account has access to will be displayed, for example:

\\10.0.0.2\share\partition1

4. You can now read and copy files from the USB directory. If the account has write access, you can also post files to the USB drive directory.

Connecting to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you must use the router's Internet port IP address rather than the local IP address.

Locating the Internet Port IP Address

1. The Router Status screen shows the Internet port IP address:Log in to the DG834GUv5 router at its default LAN address of *http://10.0.0.2* with its default user name of **admin** and default password of **admin**, or using whatever LAN address and password you have assigned.
2. Under the Maintenance section in the left navigator, click **Router Status**.
3. Record the IP address that is listed for the Internet Port. This is the IP address you can use to connect to the router remotely.

Accessing the Router's USB Drive Remotely Using FTP

You can connect to the router's USB drive using a Web browser:

1. Connect to the router by typing ftp:// and the Internet port IP address in the address field of Internet Explorer or Netscape® Navigator, for example:

ftp://10.1.65.4 If you are using dynamic DNS, you can type the DNS name rather than the IP address.

2. Type the account name and password that has access rights to the USB drive.
3. The directories of the USB drive that your account has access to will be displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connecting to the USB Drive From Your Home/Office Network

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You must be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as drag and drop, file open, or cut/paste files from:

- Microsoft Windows Start Menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer's network properties must be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networks must be enabled, as described below.

Note: In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default

.

Configuring Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right click on 'Network Neighborhood' and click Properties. File and printer sharing for Microsoft Windows should be listed. If not, click Add and follow the
installation prompts.

Note: If you have any questions on File and Printer Sharing, please contact Microsoft for assistance.

Configuring Windows 2000 and Windows XP

Right click on the network connection for your local area network. File and Printer Sharing for

Microsoft Windows should be listed. If not, click Install and follow the installation prompts.

Accessing the USB Drive from the Windows Start Menu

To access the USB Drive using Microsoft network connections, click Windows Start > Run and type:

\\ipaddress

The ipaddress entered is the local IP address or name of the router, for example, \\10.0.0.2 or \\DG834GUv5. A new Explorer window will pop up displaying the root folders your account has access to.

Accessing the USB Drive from Windows Explorer

Typing \\ipaddress or \\hostname in Windows Explorer will display the root folders granted access to on the USB drive. The hostname entered is the Host Name specified in the USB Drive Settings screen of the DG834GUv5 administrator console, for example, DG834GUv5.

Accessing the USB Drive from My Network Places

You can use Windows Network Neighborhood or Network Connections to view files on the USB drive locally. For example, to connect to the USB drive from local computers using Windows XP:

1. 1. From the Start Menu, open My Network Places.
2. Open the folder containing the files to access, for example:

share/partition1/folder1s

Appendix A
Technical Specifications

This appendix provides technical specifications for the 54 Mbps Wireless ADSL2+ Modem Router with USB Model DG834GUv5.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPPoA, or PPTP, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter	
North America:	120V AC, 60 Hz, input
United Kingdom, Australia:	240V AC, 50 Hz, input
Europe:	230V AC, 50 Hz, input
Japan:	100V AC, 50/60 Hz, input
All regions (output):	12 V DC @ 1.0A output
Physical Specifications	
Dimensions:	6.9" x 4.7" x 1.1" 175 mm x 119 mm x 28 mm
Weight:	0.7 lbs. 0.3 kg
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	ADSL, ADSL2+, Dual RJ-11, pins 2 and 3,T1.413, G.DMT, G.Lite, ITU Annex A (for the DG834G) or ITU Annex B (for the DG834GB)

AppendixB
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm